참조 안내서

AWS 관리형 정책

AWS 관리형 정책: 참조 안내서

Table of Contents

AWS 관리형 정책이란 무엇인가요? 1
정책 참조 페이지 이해 1
사용되지 않는 AWS 관리형 정책 2
AWS 관리형 정책 3
AccessAnalyzerServiceRolePolicy 43
이 정책 사용 43
정책 세부 정보 43
정책 버전 43
JSON 정책 문서 44
자세히 알아보기 46
AdministratorAccess 46
이 정책 사용 46
정책 세부 정보 46
정책 버전 46
JSON 정책 문서 47
자세히 알아보기 47
AdministratorAccess-Amplify 47
이 정책 사용 47
정책 세부 정보 47
정책 버전 48
JSON 정책 문서 48
자세히 알아보기 58
AdministratorAccess-AWSElasticBeanstalk 58
이 정책 사용 58
정책 세부 정보 59
정책 버전 59
JSON 정책 문서 59
자세히 알아보기 67
AlexaForBusinessDeviceSetup 67
이 정책 사용 67
정책 세부 정보 68
정책 버전 68
JSON 정책 문서 68
자세히 알아보기 69

AlexaForBusinessFullAccess 69
이 정책 사용 69
정책 세부 정보 69
정책 버전 69
JSON 정책 문서 69
자세히 알아보기 71
AlexaForBusinessGatewayExecution 71
이 정책 사용 71
정책 세부 정보 71
정책 버전 71
JSON 정책 문서 72
자세히 알아보기 73
AlexaForBusinessLifesizeDelegatedAccessPolicy 73
이 정책 사용 73
정책 세부 정보 73
정책 버전 73
JSON 정책 문서 73
자세히 알아보기 76
AlexaForBusinessNetworkProfileServicePolicy 76
이 정책 사용 76
정책 세부 정보 76
정책 버전 76
JSON 정책 문서 77
자세히 알아보기 77
AlexaForBusinessPolyDelegatedAccessPolicy 77
이 정책 사용 78
정책 세부 정보 78
정책 버전 78
JSON 정책 문서 78
자세히 알아보기 80
AlexaForBusinessReadOnlyAccess 80
이 정책 사용 80
정책 세부 정보 80
정책 버전 80
JSON 정책 문서 81
자세히 알아보기 81

AmazonAPIGatewayAdministrator 81
이 정책 사용 81
정책 세부 정보 82
정책 버전 82
JSON 정책 문서 82
자세히 알아보기 82
AmazonAPIGatewayInvokeFullAccess 83
이 정책 사용 83
정책 세부 정보 83
정책 버전 83
JSON 정책 문서 83
자세히 알아보기 84
AmazonAPIGatewayPushToCloudWatchLogs 84
이 정책 사용 84
정책 세부 정보 84
정책 버전 84
JSON 정책 문서 84
자세히 알아보기 85
AmazonAppFlowFullAccess 85
이 정책 사용 85
정책 세부 정보 85
정책 버전 86
JSON 정책 문서 86
자세히 알아보기 89
AmazonAppFlowReadOnlyAccess 89
이 정책 사용 89
정책 세부 정보 89
정책 버전 89
JSON 정책 문서 89
자세히 알아보기 90
AmazonAppStreamFullAccess 90
이 정책 사용 90
정책 세부 정보 90
정책 버전 91
JSON 정책 문서 91
자세히 알아보기 93

AmazonAppStreamPCAAccess 93
이 정책 사용 93
정책 세부 정보 93
정책 버전 93
JSON 정책 문서 93
자세히 알아보기 94
AmazonAppStreamReadOnlyAccess 94
이 정책 사용 94
정책 세부 정보 94
정책 버전 95
JSON 정책 문서 95
자세히 알아보기 95
AmazonAppStreamServiceAccess 95
이 정책 사용 96
정책 세부 정보 96
정책 버전 96
JSON 정책 문서 96
자세히 알아보기 97
AmazonAthenaFullAccess 97
이 정책 사용 98
정책 세부 정보 98
정책 버전 98
JSON 정책 문서 98
자세히 알아보기 101
AmazonAugmentedAIFullAccess 102
이 정책 사용 102
정책 세부 정보 102
정책 버전 102
JSON 정책 문서 102
자세히 알아보기 103
AmazonAugmentedAIHumanLoopFullAccess 104
이 정책 사용 104
정책 세부 정보 104
정책 버전 104
JSON 정책 문서 104
자세히 알아보기 105

AmazonAugmentedAIIntegratedAPIAccess 105
이 정책 사용 105
정책 세부 정보 105
정책 버전 105
JSON 정책 문서 105
자세히 알아보기 107
AmazonBedrockFullAccess 107
이 정책 사용 107
정책 세부 정보 107
정책 버전 107
JSON 정책 문서 108
자세히 알아보기 109
AmazonBedrockReadOnly 109
이 정책 사용 109
정책 세부 정보 109
정책 버전 109
JSON 정책 문서 110
자세히 알아보기 110
AmazonBraketFullAccess 111
이 정책 사용 111
정책 세부 정보 111
정책 버전 111
JSON 정책 문서 111
자세히 알아보기 115
AmazonBraketJobsExecutionPolicy 116
이 정책 사용 116
정책 세부 정보 116
정책 버전 116
JSON 정책 문서 116
자세히 알아보기 119
AmazonBraketServiceRolePolicy 119
이 정책 사용 119
정책 세부 정보 119
정책 버전 119
JSON 정책 문서 120
자세히 알아보기 120

AmazonChimeFullAccess 120
이 정책 사용 121
정책 세부 정보 121
정책 버전 121
JSON 정책 문서 121
자세히 알아보기 123
AmazonChimeReadOnly 123
이 정책 사용 123
정책 세부 정보 124
정책 버전 124
JSON 정책 문서 124
자세히 알아보기 124
AmazonChimeSDK 125
이 정책 사용 125
정책 세부 정보 125
정책 버전 125
JSON 정책 문서 125
자세히 알아보기 126
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 127
이 정책 사용 127
정책 세부 정보 127
정책 버전 127
JSON 정책 문서 127
자세히 알아보기 128
AmazonChimeSDKMessagingServiceRolePolicy 129
이 정책 사용 129
정책 세부 정보 129
정책 버전 129
JSON 정책 문서 129
자세히 알아보기 130
AmazonChimeServiceRolePolicy 130
이 정책 사용 130
정책 세부 정보 130
정책 버전 131
JSON 정책 문서 131
자세히 알아보기 131

AmazonChimeTranscriptionServiceLinkedRolePolicy 132
이 정책 사용 132
정책 세부 정보 132
정책 버전 132
JSON 정책 문서 132
자세히 알아보기 133
AmazonChimeUserManagement 133
이 정책 사용 133
정책 세부 정보 133
정책 버전 133
JSON 정책 문서 134
자세히 알아보기 135
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 135
이 정책 사용 135
정책 세부 정보 135
정책 버전 135
JSON 정책 문서 136
자세히 알아보기 137
AmazonCloudDirectoryFullAccess 138
이 정책 사용 138
정책 세부 정보 138
정책 버전 138
JSON 정책 문서 138
자세히 알아보기 139
AmazonCloudDirectoryReadOnlyAccess 139
이 정책 사용 139
정책 세부 정보 139
정책 버전 139
JSON 정책 문서 139
자세히 알아보기 140
AmazonCloudWatchEvidentlyFullAccess 140
이 정책 사용 140
정책 세부 정보 140
정책 버전 141
JSON 정책 문서 141
자세히 알아보기 143

AmazonCloudWatchEvidentlyReadOnlyAccess 144
이 정책 사용 144
정책 세부 정보 144
정책 버전 144
JSON 정책 문서 144
자세히 알아보기 145
AmazonCloudWatchEvidentlyServiceRolePolicy 145
이 정책 사용 145
정책 세부 정보 145
정책 버전 145
JSON 정책 문서 146
자세히 알아보기 147
AmazonCloudWatchRUMFullAccess 147
이 정책 사용 147
정책 세부 정보 147
정책 버전 148
JSON 정책 문서 148
자세히 알아보기 150
AmazonCloudWatchRUMReadOnlyAccess 151
이 정책 사용 151
정책 세부 정보 151
정책 버전 151
JSON 정책 문서 151
자세히 알아보기 152
AmazonCloudWatchRUMServiceRolePolicy 152
이 정책 사용 152
정책 세부 정보 152
정책 버전 152
JSON 정책 문서 153
자세히 알아보기 153
AmazonCodeCatalystFullAccess 153
이 정책 사용 154
정책 세부 정보 154
정책 버전 154
JSON 정책 문서 154
자세히 알아보기 155

AmazonCodeCatalystReadOnlyAccess 155
이 정책 사용 155
정책 세부 정보 155
정책 버전 155
JSON 정책 문서 156
자세히 알아보기 156
AmazonCodeCatalystSupportAccess 156
이 정책 사용 156
정책 세부 정보 156
정책 버전 157
JSON 정책 문서 157
자세히 알아보기 158
AmazonCodeGuruProfilerAgentAccess 158
이 정책 사용 158
정책 세부 정보 158
정책 버전 158
JSON 정책 문서 158
자세히 알아보기 159
AmazonCodeGuruProfilerFullAccess 159
이 정책 사용 159
정책 세부 정보 159
정책 버전 160
JSON 정책 문서 160
자세히 알아보기 160
AmazonCodeGuruProfilerReadOnlyAccess 161
이 정책 사용 161
정책 세부 정보 161
정책 버전 161
JSON 정책 문서 161
자세히 알아보기 162
AmazonCodeGuruReviewerFullAccess 162
이 정책 사용 162
정책 세부 정보 162
정책 버전 162
JSON 정책 문서 163
자세히 알아보기 165

AmazonCodeGuruReviewerReadOnlyAccess 165
이 정책 사용 166
정책 세부 정보 166
정책 버전 166
JSON 정책 문서 166
자세히 알아보기 167
AmazonCodeGuruReviewerServiceRolePolicy 167
이 정책 사용 167
정책 세부 정보 167
정책 버전 167
JSON 정책 문서 167
자세히 알아보기 169
AmazonCodeGuruSecurityFullAccess 170
이 정책 사용 170
정책 세부 정보 170
정책 버전 170
JSON 정책 문서 170
자세히 알아보기 171
AmazonCodeGuruSecurityScanAccess 171
이 정책 사용 171
정책 세부 정보 171
정책 버전 171
JSON 정책 문서 171
자세히 알아보기 172
AmazonCognitoDeveloperAuthenticatedIdentities 172
이 정책 사용 172
정책 세부 정보 172
정책 버전 173
JSON 정책 문서 173
자세히 알아보기 173
AmazonCognitoIdpEmailServiceRolePolicy 173
이 정책 사용 174
정책 세부 정보 174
정책 버전 174
JSON 정책 문서 174
자세히 알아보기 175

AmazonCognitoIdpServiceRolePolicy 175
이 정책 사용 175
정책 세부 정보 175
정책 버전 175
JSON 정책 문서 175
자세히 알아보기 176
AmazonCognitoPowerUser 176
이 정책 사용 176
정책 세부 정보 176
정책 버전 176
JSON 정책 문서 177
자세히 알아보기 178
AmazonCognitoReadOnly 178
이 정책 사용 178
정책 세부 정보 178
정책 버전 179
JSON 정책 문서 179
자세히 알아보기 179
AmazonCognitoUnAuthedIdentitiesSessionPolicy 180
이 정책 사용 180
정책 세부 정보 180
정책 버전 180
JSON 정책 문서 181
자세히 알아보기 181
AmazonCognitoUnauthenticatedIdentities 181
이 정책 사용 182
정책 세부 정보 182
정책 버전 182
JSON 정책 문서 182
자세히 알아보기 182
AmazonConnect_FullAccess 183
이 정책 사용 183
정책 세부 정보 183
정책 버전 183
JSON 정책 문서 183
자세히 알아보기 186

AmazonConnectCampaignsServiceLinkedRolePolicy 186
이 정책 사용 186
정책 세부 정보 186
정책 버전 186
JSON 정책 문서 187
자세히 알아보기 187
AmazonConnectReadOnlyAccess 187
이 정책 사용 187
정책 세부 정보 188
정책 버전 188
JSON 정책 문서 188
자세히 알아보기 189
AmazonConnectServiceLinkedRolePolicy 189
이 정책 사용 189
정책 세부 정보 189
정책 버전 189
JSON 정책 문서 189
자세히 알아보기 194
AmazonConnectSynchronizationServiceRolePolicy 194
이 정책 사용 194
정책 세부 정보 194
정책 버전 195
JSON 정책 문서 195
자세히 알아보기 197
AmazonConnectVoiceIDFullAccess 197
이 정책 사용 197
정책 세부 정보 197
정책 버전 197
JSON 정책 문서 198
자세히 알아보기 198
AmazonDataZoneDomainExecutionRolePolicy 198
이 정책 사용 198
정책 세부 정보 198
정책 버전 199
JSON 정책 문서 199
자세히 알아보기 202

AmazonDataZoneEnvironmentRolePermissionsBoundary 202
이 정책 사용 202
정책 세부 정보 202
정책 버전 202
JSON 정책 문서 203
자세히 알아보기 215
AmazonDataZoneFullAccess 216
이 정책 사용 216
정책 세부 정보 216
정책 버전 216
JSON 정책 문서 216
자세히 알아보기 219
AmazonDataZoneFullUserAccess 220
이 정책 사용 220
정책 세부 정보 220
정책 버전 220
JSON 정책 문서 220
자세히 알아보기 223
AmazonDataZoneGlueManageAccessRolePolicy 223
이 정책 사용 223
정책 세부 정보 223
정책 버전 224
JSON 정책 문서 224
자세히 알아보기 227
AmazonDataZonePortalFullAccessPolicy 228
이 정책 사용 228
정책 세부 정보 228
정책 버전 228
JSON 정책 문서 228
자세히 알아보기 229
AmazonDataZonePreviewConsoleFullAccess 229
이 정책 사용 229
정책 세부 정보 229
정책 버전 229
JSON 정책 문서 229
자세히 알아보기 231

AmazonDataZoneProjectDeploymentPermissionsBoundary 232
이 정책 사용 232
정책 세부 정보 232
정책 버전 232
JSON 정책 문서 232
자세히 알아보기 240
AmazonDataZoneProjectRolePermissionsBoundary 240
이 정책 사용 241
정책 세부 정보 241
정책 버전 241
JSON 정책 문서 241
자세히 알아보기 248
AmazonDataZoneRedshiftGlueProvisioningPolicy 248
이 정책 사용 249
정책 세부 정보 249
정책 버전 249
JSON 정책 문서 249
자세히 알아보기 257
AmazonDataZoneRedshiftManageAccessRolePolicy 257
이 정책 사용 257
정책 세부 정보 257
정책 버전 258
JSON 정책 문서 258
자세히 알아보기 260
AmazonDetectiveFullAccess 260
이 정책 사용 260
정책 세부 정보 260
정책 버전 261
JSON 정책 문서 261
자세히 알아보기 262
AmazonDetectiveInvestigatorAccess 262
이 정책 사용 262
정책 세부 정보 262
정책 버전 262
JSON 정책 문서 263
자세히 알아보기 264

AmazonDetectiveMemberAccess 264
이 정책 사용 264
정책 세부 정보 264
정책 버전 265
JSON 정책 문서 265
자세히 알아보기 265
AmazonDetectiveOrganizationsAccess 266
이 정책 사용 266
정책 세부 정보 266
정책 버전 266
JSON 정책 문서 266
자세히 알아보기 268
AmazonDetectiveServiceLinkedRolePolicy 268
이 정책 사용 268
정책 세부 정보 268
정책 버전 269
JSON 정책 문서 269
자세히 알아보기 269
AmazonDevOpsGuruConsoleFullAccess 269
이 정책 사용 270
정책 세부 정보 270
정책 버전 270
JSON 정책 문서 270
자세히 알아보기 272
AmazonDevOpsGuruFullAccess 273
이 정책 사용 273
정책 세부 정보 273
정책 버전 273
JSON 정책 문서 273
자세히 알아보기 275
AmazonDevOpsGuruOrganizationsAccess 276
이 정책 사용 276
정책 세부 정보 276
정책 버전 276
JSON 정책 문서 276
자세히 알아보기 278

AmazonDevOpsGuruReadOnlyAccess 278
이 정책 사용 278
정책 세부 정보 278
정책 버전 278
JSON 정책 문서 278
자세히 알아보기 280
AmazonDevOpsGuruServiceRolePolicy 281
이 정책 사용 281
정책 세부 정보 281
정책 버전 281
JSON 정책 문서 281
자세히 알아보기 285
AmazonDMSCloudWatchLogsRole 285
이 정책 사용 286
정책 세부 정보 286
정책 버전 286
JSON 정책 문서 286
자세히 알아보기 288
AmazonDMSRedshiftS3Role 288
이 정책 사용 288
정책 세부 정보 288
정책 버전 288
JSON 정책 문서 288
자세히 알아보기 289
AmazonDMSVPCManagementRole 289
이 정책 사용 289
정책 세부 정보 290
정책 버전 290
JSON 정책 문서 290
자세히 알아보기 290
AmazonDocDB-ElasticServiceRolePolicy 291
이 정책 사용 291
정책 세부 정보 291
정책 버전 291
JSON 정책 문서 291
자세히 알아보기 292

AmazonDocDBConsoleFullAccess 292
이 정책 사용 292
정책 세부 정보 292
정책 버전 293
JSON 정책 문서 293
자세히 알아보기 297
AmazonDocDBElasticFullAccess 297
이 정책 사용 297
정책 세부 정보 297
정책 버전 298
JSON 정책 문서 298
자세히 알아보기 301
AmazonDocDBElasticReadOnlyAccess 301
이 정책 사용 301
정책 세부 정보 301
정책 버전 301
JSON 정책 문서 302
자세히 알아보기 302
AmazonDocDBFullAccess 303
이 정책 사용 303
정책 세부 정보 303
정책 버전 303
JSON 정책 문서 303
자세히 알아보기 306
AmazonDocDBReadOnlyAccess 306
이 정책 사용 306
정책 세부 정보 306
정책 버전 307
JSON 정책 문서 307
자세히 알아보기 309
AmazonDRSVPCManagement 309
이 정책 사용 309
정책 세부 정보 309
정책 버전 309
JSON 정책 문서 309
자세히 알아보기 310

AmazonDynamoDBFullAccess 310
이 정책 사용 310
정책 세부 정보 310
정책 버전 311
JSON 정책 문서 311
자세히 알아보기 313
AmazonDynamoDBFullAccesswithDataPipeline 314
이 정책 사용 314
정책 세부 정보 314
정책 버전 314
JSON 정책 문서 314
자세히 알아보기 316
AmazonDynamoDBReadOnlyAccess 317
이 정책 사용 317
정책 세부 정보 317
정책 버전 317
JSON 정책 문서 317
자세히 알아보기 319
AmazonEBSCSIDriverPolicy 319
이 정책 사용 319
정책 세부 정보 319
정책 버전 319
JSON 정책 문서 320
자세히 알아보기 323
AmazonEC2ContainerRegistryFullAccess 323
이 정책 사용 323
정책 세부 정보 323
정책 버전 323
JSON 정책 문서 324
자세히 알아보기 324
AmazonEC2ContainerRegistryPowerUser 325
이 정책 사용 325
정책 세부 정보 325
정책 버전 325
JSON 정책 문서 325
자세히 알아보기 326

AmazonEC2ContainerRegistryReadOnly 326
이 정책 사용 326
정책 세부 정보 326
정책 버전 327
JSON 정책 문서 327
자세히 알아보기 327
AmazonEC2ContainerServiceAutoscaleRole 328
이 정책 사용 328
정책 세부 정보 328
정책 버전 328
JSON 정책 문서 328
자세히 알아보기 329
AmazonEC2ContainerServiceEventsRole 329
이 정책 사용 329
정책 세부 정보 329
정책 버전 330
JSON 정책 문서 330
자세히 알아보기 331
AmazonEC2ContainerServiceforEC2Role 331
이 정책 사용 331
정책 세부 정보 331
정책 버전 331
JSON 정책 문서 332
자세히 알아보기 333
AmazonEC2ContainerServiceRole 333
이 정책 사용 333
정책 세부 정보 333
정책 버전 333
JSON 정책 문서 333
자세히 알아보기 334
AmazonEC2FullAccess 334
이 정책 사용 334
정책 세부 정보 334
정책 버전 335
JSON 정책 문서 335
자세히 알아보기 336

AmazonEC2ReadOnlyAccess 336
이 정책 사용 336
정책 세부 정보 336
정책 버전 337
JSON 정책 문서 337
자세히 알아보기 338
AmazonEC2RoleforAWSCodeDeploy 338
이 정책 사용 338
정책 세부 정보 338
정책 버전 338
JSON 정책 문서 338
자세히 알아보기 339
AmazonEC2RoleforAWSCodeDeployLimited 339
이 정책 사용 339
정책 세부 정보 339
정책 버전 340
JSON 정책 문서 340
자세히 알아보기 340
AmazonEC2RoleforDataPipelineRole 341
이 정책 사용 341
정책 세부 정보 341
정책 버전 341
JSON 정책 문서 341
자세히 알아보기 342
AmazonEC2RoleforSSM 342
이 정책 사용 342
정책 세부 정보 343
정책 버전 343
JSON 정책 문서 343
자세히 알아보기 345
AmazonEC2RolePolicyForLaunchWizard 345
이 정책 사용 346
정책 세부 정보 346
정책 버전 346
JSON 정책 문서 346
자세히 알아보기 350

AmazonEC2SpotFleetAutoscaleRole 350
이 정책 사용 350
정책 세부 정보 350
정책 버전 351
JSON 정책 문서 351
자세히 알아보기 352
AmazonEC2SpotFleetTaggingRole 352
이 정책 사용 352
정책 세부 정보 352
정책 버전 352
JSON 정책 문서 353
자세히 알아보기 354
AmazonECS_FullAccess 354
이 정책 사용 354
정책 세부 정보 354
정책 버전 355
JSON 정책 문서 355
자세히 알아보기 360
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 360
이 정책 사용 360
정책 세부 정보 361
정책 버전 361
JSON 정책 문서 361
자세히 알아보기 363
AmazonECSInfrastructureRolePolicyForVolumes 363
이 정책 사용 364
정책 세부 정보 364
정책 버전 364
JSON 정책 문서 364
자세히 알아보기 366
AmazonECSServiceRolePolicy 366
이 정책 사용 366
정책 세부 정보 366
정책 버전 367
JSON 정책 문서 367
자세히 알아보기 372

AmazonECSTaskExecutionRolePolicy 372
이 정책 사용 372
정책 세부 정보 372
정책 버전 372
JSON 정책 문서 372
자세히 알아보기 373
AmazonEFSCSIDriverPolicy 373
이 정책 사용 373
정책 세부 정보 373
정책 버전 374
JSON 정책 문서 374
자세히 알아보기 375
AmazonEKS_CNI_Policy 376
이 정책 사용 376
정책 세부 정보 376
정책 버전 376
JSON 정책 문서 376
자세히 알아보기 377
AmazonEKSClusterPolicy 377
이 정책 사용 378
정책 세부 정보 378
정책 버전 378
JSON 정책 문서 378
자세히 알아보기 380
AmazonEKSConnectorServiceRolePolicy 380
이 정책 사용 380
정책 세부 정보 380
정책 버전 381
JSON 정책 문서 381
자세히 알아보기 383
AmazonEKSFargatePodExecutionRolePolicy 383
이 정책 사용 383
정책 세부 정보 383
정책 버전 383
JSON 정책 문서 383
자세히 알아보기 384

AmazonEKSForFargateServiceRolePolicy 384
이 정책 사용 384
정책 세부 정보 384
정책 버전 385
JSON 정책 문서 385
자세히 알아보기 385
AmazonEKSLocalOutpostClusterPolicy 386
이 정책 사용 386
정책 세부 정보 386
정책 버전 386
JSON 정책 문서 386
자세히 알아보기 388
AmazonEKSLocalOutpostServiceRolePolicy 388
이 정책 사용 388
정책 세부 정보 388
정책 버전 389
JSON 정책 문서 389
자세히 알아보기 394
AmazonEKSServicePolicy 395
이 정책 사용 395
정책 세부 정보 395
정책 버전 395
JSON 정책 문서 395
자세히 알아보기 397
AmazonEKSServiceRolePolicy 397
이 정책 사용 397
정책 세부 정보 397
정책 버전 398
JSON 정책 문서 398
자세히 알아보기 400
AmazonEKSVPCResourceController 400
이 정책 사용 400
정책 세부 정보 400
정책 버전 401
JSON 정책 문서 401
자세히 알아보기 401

AmazonEKSWorkerNodePolicy 402
이 정책 사용 402
정책 세부 정보 402
정책 버전 402
JSON 정책 문서 402
자세히 알아보기 403
AmazonElastiCacheFullAccess 403
이 정책 사용 403
정책 세부 정보 403
정책 버전 404
JSON 정책 문서 404
자세히 알아보기 407
AmazonElastiCacheReadOnlyAccess 407
이 정책 사용 407
정책 세부 정보 407
정책 버전 408
JSON 정책 문서 408
자세히 알아보기 408
AmazonElasticContainerRegistryPublicFullAccess 408
이 정책 사용 408
정책 세부 정보 409
정책 버전 409
JSON 정책 문서 409
자세히 알아보기 409
AmazonElasticContainerRegistryPublicPowerUser 410
이 정책 사용 410
정책 세부 정보 410
정책 버전 410
JSON 정책 문서 410
자세히 알아보기 411
AmazonElasticContainerRegistryPublicReadOnly 411
이 정책 사용 411
정책 세부 정보 411
정책 버전 412
JSON 정책 문서 412
자세히 알아보기 412

AmazonElasticFileSystemClientFullAccess 413
이 정책 사용 413
정책 세부 정보 413
정책 버전 413
JSON 정책 문서 413
자세히 알아보기 414
AmazonElasticFileSystemClientReadOnlyAccess 414
이 정책 사용 414
정책 세부 정보 414
정책 버전 414
JSON 정책 문서 415
자세히 알아보기 415
AmazonElasticFileSystemClientReadWriteAccess 415
이 정책 사용 415
정책 세부 정보 415
정책 버전 416
JSON 정책 문서 416
자세히 알아보기 416
AmazonElasticFileSystemFullAccess 416
이 정책 사용 417
정책 세부 정보 417
정책 버전 417
JSON 정책 문서 417
자세히 알아보기 419
AmazonElasticFileSystemReadOnlyAccess 419
이 정책 사용 419
정책 세부 정보 419
정책 버전 419
JSON 정책 문서 420
자세히 알아보기 420
AmazonElasticFileSystemServiceRolePolicy 421
이 정책 사용 421
정책 세부 정보 421
정책 버전 421
JSON 정책 문서 421
자세히 알아보기 423

AmazonElasticFileSystemsUtils 424
이 정책 사용 424
정책 세부 정보 424
정책 버전 424
JSON 정책 문서 424
자세히 알아보기 426
AmazonElasticMapReduceEditorsRole 426
이 정책 사용 426
정책 세부 정보 426
정책 버전 427
JSON 정책 문서 427
자세히 알아보기 428
AmazonElasticMapReduceforAutoScalingRole 428
이 정책 사용 428
정책 세부 정보 428
정책 버전 429
JSON 정책 문서 429
자세히 알아보기 429
AmazonElasticMapReduceforEC2Role 429
이 정책 사용 430
정책 세부 정보 430
정책 버전 430
JSON 정책 문서 430
자세히 알아보기 431
AmazonElasticMapReduceFullAccess 432
이 정책 사용 432
정책 세부 정보 432
정책 버전 432
JSON 정책 문서 432
자세히 알아보기 434
AmazonElasticMapReducePlacementGroupPolicy 434
이 정책 사용 434
정책 세부 정보 434
정책 버전 435
JSON 정책 문서 435
자세히 알아보기 435

AmazonElasticMapReduceReadOnlyAccess 436
이 정책 사용 436
정책 세부 정보 436
정책 버전 436
JSON 정책 문서 436
자세히 알아보기 437
AmazonElasticMapReduceRole 437
이 정책 사용 437
정책 세부 정보 437
정책 버전 437
JSON 정책 문서 438
자세히 알아보기 440
AmazonElasticsearchServiceRolePolicy 440
이 정책 사용 440
정책 세부 정보 440
정책 버전 441
JSON 정책 문서 441
자세히 알아보기 443
AmazonElasticTranscoder_FullAccess 444
이 정책 사용 444
정책 세부 정보 444
정책 버전 444
JSON 정책 문서 444
자세히 알아보기 445
AmazonElasticTranscoder_JobsSubmitter 445
이 정책 사용 445
정책 세부 정보 446
정책 버전 446
JSON 정책 문서 446
자세히 알아보기 446
AmazonElasticTranscoder_ReadOnlyAccess 447
이 정책 사용 447
정책 세부 정보 447
정책 버전 447
JSON 정책 문서 447
자세히 알아보기 448

AmazonElasticTranscoderRole 448
이 정책 사용 448
정책 세부 정보 448
정책 버전 448
JSON 정책 문서 449
자세히 알아보기 449
AmazonEMRCleanupPolicy 450
이 정책 사용 450
정책 세부 정보 450
정책 버전 450
JSON 정책 문서 450
자세히 알아보기 451
AmazonEMRContainersServiceRolePolicy 451
이 정책 사용 451
정책 세부 정보 451
정책 버전 452
JSON 정책 문서 452
자세히 알아보기 453
AmazonEMRFullAccessPolicy_v2 453
이 정책 사용 453
정책 세부 정보 453
정책 버전 453
JSON 정책 문서 454
자세히 알아보기 457
AmazonEMRReadOnlyAccessPolicy_v2 457
이 정책 사용 457
정책 세부 정보 457
정책 버전 458
JSON 정책 문서 458
자세히 알아보기 459
AmazonEMRServerlessServiceRolePolicy 459
이 정책 사용 459
정책 세부 정보 459
정책 버전 460
JSON 정책 문서 460
자세히 알아보기 461

AmazonEMRServicePolicy_v2 461
이 정책 사용 461
정책 세부 정보 461
정책 버전 461
JSON 정책 문서 462
자세히 알아보기 469
AmazonESCognitoAccess 469
이 정책 사용 469
정책 세부 정보 470
정책 버전 470
JSON 정책 문서 470
자세히 알아보기 471
AmazonESFullAccess 471
이 정책 사용 471
정책 세부 정보 471
정책 버전 472
JSON 정책 문서 472
자세히 알아보기 472
AmazonESReadOnlyAccess 472
이 정책 사용 472
정책 세부 정보 473
정책 버전 473
JSON 정책 문서 473
자세히 알아보기 473
AmazonEventBridgeApiDestinationsServiceRolePolicy 474
이 정책 사용 474
정책 세부 정보 474
정책 버전 474
JSON 정책 문서 474
자세히 알아보기 475
AmazonEventBridgeFullAccess 475
이 정책 사용 475
정책 세부 정보 475
정책 버전 475
JSON 정책 문서 476
자세히 알아보기 478

AmazonEventBridgePipesFullAccess 478
이 정책 사용 478
정책 세부 정보 478
정책 버전 478
JSON 정책 문서 478
자세히 알아보기 479
AmazonEventBridgePipesOperatorAccess 479
이 정책 사용 479
정책 세부 정보 479
정책 버전 480
JSON 정책 문서 480
자세히 알아보기 480
AmazonEventBridgePipesReadOnlyAccess 481
이 정책 사용 481
정책 세부 정보 481
정책 버전 481
JSON 정책 문서 481
자세히 알아보기 482
AmazonEventBridgeReadOnlyAccess 482
이 정책 사용 482
정책 세부 정보 482
정책 버전 482
JSON 정책 문서 482
자세히 알아보기 484
AmazonEventBridgeSchedulerFullAccess 484
이 정책 사용 484
정책 세부 정보 484
정책 버전 484
JSON 정책 문서 485
자세히 알아보기 485
AmazonEventBridgeSchedulerReadOnlyAccess 485
이 정책 사용 486
정책 세부 정보 486
정책 버전 486
JSON 정책 문서 486
자세히 알아보기 487

AmazonEventBridgeSchemasFullAccess 487
이 정책 사용 487
정책 세부 정보 487
정책 버전 487
JSON 정책 문서 487
자세히 알아보기 488
AmazonEventBridgeSchemasReadOnlyAccess 489
이 정책 사용 489
정책 세부 정보 489
정책 버전 489
JSON 정책 문서 489
자세히 알아보기 490
AmazonEventBridgeSchemasServiceRolePolicy 490
이 정책 사용 490
정책 세부 정보 490
정책 버전 491
JSON 정책 문서 491
자세히 알아보기 491
AmazonFISServiceRolePolicy 491
이 정책 사용 492
정책 세부 정보 492
정책 버전 492
JSON 정책 문서 492
자세히 알아보기 494
AmazonForecastFullAccess 494
이 정책 사용 494
정책 세부 정보 494
정책 버전 494
JSON 정책 문서 494
자세히 알아보기 495
AmazonFraudDetectorFullAccessPolicy 495
이 정책 사용 495
정책 세부 정보 496
정책 버전 496
JSON 정책 문서 496
자세히 알아보기 497

AmazonFreeRTOSFullAccess 497
이 정책 사용 497
정책 세부 정보 498
정책 버전 498
JSON 정책 문서 498
자세히 알아보기 498
AmazonFreeRTOSOTAUpdate 499
이 정책 사용 499
정책 세부 정보 499
정책 버전 499
JSON 정책 문서 499
자세히 알아보기 501
AmazonFSxConsoleFullAccess 501
이 정책 사용 501
정책 세부 정보 501
정책 버전 501
JSON 정책 문서 501
자세히 알아보기 505
AmazonFSxConsoleReadOnlyAccess 505
이 정책 사용 505
정책 세부 정보 505
정책 버전 505
JSON 정책 문서 506
자세히 알아보기 506
AmazonFSxFullAccess 507
이 정책 사용 507
정책 세부 정보 507
정책 버전 507
JSON 정책 문서 507
자세히 알아보기 511
AmazonFSxReadOnlyAccess 511
이 정책 사용 512
정책 세부 정보 512
정책 버전 512
JSON 정책 문서 512
자세히 알아보기 512

AmazonFSxServiceRolePolicy 513
이 정책 사용 513
정책 세부 정보 513
정책 버전 513
JSON 정책 문서 513
자세히 알아보기 516
AmazonGlacierFullAccess 516
이 정책 사용 516
정책 세부 정보 516
정책 버전 517
JSON 정책 문서 517
자세히 알아보기 517
AmazonGlacierReadOnlyAccess 517
이 정책 사용 517
정책 세부 정보 518
정책 버전 518
JSON 정책 문서 518
자세히 알아보기 519
AmazonGrafanaAthenaAccess 519
이 정책 사용 519
정책 세부 정보 519
정책 버전 519
JSON 정책 문서 519
자세히 알아보기 521
AmazonGrafanaCloudWatchAccess 521
이 정책 사용 521
정책 세부 정보 522
정책 버전 522
JSON 정책 문서 522
자세히 알아보기 523
AmazonGrafanaRedshiftAccess 524
이 정책 사용 524
정책 세부 정보 524
정책 버전 524
JSON 정책 문서 524
자세히 알아보기 525

AmazonGrafanaServiceLinkedRolePolicy 526
이 정책 사용 526
정책 세부 정보 526
정책 버전 526
JSON 정책 문서 526
자세히 알아보기 528
AmazonGuardDutyFullAccess 528
이 정책 사용 528
정책 세부 정보 528
정책 버전 528
JSON 정책 문서 528
자세히 알아보기 530
AmazonGuardDutyMalwareProtectionServiceRolePolicy 530
이 정책 사용 530
정책 세부 정보 530
정책 버전 530
JSON 정책 문서 531
자세히 알아보기 535
AmazonGuardDutyReadOnlyAccess 535
이 정책 사용 535
정책 세부 정보 535
정책 버전 536
JSON 정책 문서 536
자세히 알아보기 536
AmazonGuardDutyServiceRolePolicy 537
이 정책 사용 537
정책 세부 정보 537
정책 버전 537
JSON 정책 문서 537
자세히 알아보기 542
AmazonHealthLakeFullAccess 542
이 정책 사용 542
정책 세부 정보 542
정책 버전 543
JSON 정책 문서 543
자세히 알아보기 543

AmazonHealthLakeReadOnlyAccess 544
이 정책 사용 544
정책 세부 정보 544
정책 버전 544
JSON 정책 문서 544
자세히 알아보기 545
AmazonHoneycodeFullAccess 545
이 정책 사용 545
정책 세부 정보 545
정책 버전 545
JSON 정책 문서 546
자세히 알아보기 546
AmazonHoneycodeReadOnlyAccess 546
이 정책 사용 546
정책 세부 정보 546
정책 버전 547
JSON 정책 문서 547
자세히 알아보기 547
AmazonHoneycodeServiceRolePolicy 548
이 정책 사용 548
정책 세부 정보 548
정책 버전 548
JSON 정책 문서 548
자세히 알아보기 549
AmazonHoneycodeTeamAssociationFullAccess 549
이 정책 사용 549
정책 세부 정보 549
정책 버전 549
JSON 정책 문서 549
자세히 알아보기 550
AmazonHoneycodeTeamAssociationReadOnlyAccess 550
이 정책 사용 550
정책 세부 정보 550
정책 버전 551
JSON 정책 문서 551
자세히 알아보기 551

AmazonHoneycodeWorkbookFullAccess 551
이 정책 사용 551
정책 세부 정보 552
정책 버전 552
JSON 정책 문서 552
자세히 알아보기 553
AmazonHoneycodeWorkbookReadOnlyAccess 553
이 정책 사용 553
정책 세부 정보 553
정책 버전 553
JSON 정책 문서 553
자세히 알아보기 554
AmazonInspector2AgentlessServiceRolePolicy 554
이 정책 사용 554
정책 세부 정보 554
정책 버전 555
JSON 정책 문서 555
자세히 알아보기 558
AmazonInspector2FullAccess 559
이 정책 사용 559
정책 세부 정보 559
정책 버전 559
JSON 정책 문서 559
자세히 알아보기 560
AmazonInspector2ManagedCisPolicy 560
이 정책 사용 561
정책 세부 정보 561
정책 버전 561
JSON 정책 문서 561
자세히 알아보기 562
AmazonInspector2ReadOnlyAccess 562
이 정책 사용 562
정책 세부 정보 562
정책 버전 562
JSON 정책 문서 562
자세히 알아보기 563

AmazonInspector2ServiceRolePolicy 563
이 정책 사용 563
정책 세부 정보 563
정책 버전 564
JSON 정책 문서 564
자세히 알아보기 570
AmazonInspectorFullAccess 570
이 정책 사용 571
정책 세부 정보 571
정책 버전 571
JSON 정책 문서 571
자세히 알아보기 572
AmazonInspectorReadOnlyAccess 572
이 정책 사용 572
정책 세부 정보 573
정책 버전 573
JSON 정책 문서 573
자세히 알아보기 574
AmazonInspectorServiceRolePolicy 574
이 정책 사용 574
정책 세부 정보 574
정책 버전 574
JSON 정책 문서 574
자세히 알아보기 576
AmazonKendraFullAccess 576
이 정책 사용 576
정책 세부 정보 576
정책 버전 576
JSON 정책 문서 577
자세히 알아보기 578
AmazonKendraReadOnlyAccess 579
이 정책 사용 579
정책 세부 정보 579
정책 버전 579
JSON 정책 문서 579
자세히 알아보기 580

AmazonKeyspacesFullAccess 580
이 정책 사용 580
정책 세부 정보 580
정책 버전 580
JSON 정책 문서 580
자세히 알아보기 582
AmazonKeyspacesReadOnlyAccess 583
이 정책 사용 583
정책 세부 정보 583
정책 버전 583
JSON 정책 문서 583
자세히 알아보기 584
AmazonKeyspacesReadOnlyAccess_v2 584
이 정책 사용 584
정책 세부 정보 584
정책 버전 585
JSON 정책 문서 585
자세히 알아보기 586
AmazonKinesisAnalyticsFullAccess 586
이 정책 사용 586
정책 세부 정보 586
정책 버전 586
JSON 정책 문서 586
자세히 알아보기 588
AmazonKinesisAnalyticsReadOnly 588
이 정책 사용 588
정책 세부 정보 588
정책 버전 588
JSON 정책 문서 589
자세히 알아보기 590
AmazonKinesisFirehoseFullAccess 590
이 정책 사용 590
정책 세부 정보 590
정책 버전 591
JSON 정책 문서 591
자세히 알아보기 591

AmazonKinesisFirehoseReadOnlyAccess 591
이 정책 사용 591
정책 세부 정보 592
정책 버전 592
JSON 정책 문서 592
자세히 알아보기 592
AmazonKinesisFullAccess 593
이 정책 사용 593
정책 세부 정보 593
정책 버전 593
JSON 정책 문서 593
자세히 알아보기 594
AmazonKinesisReadOnlyAccess 594
이 정책 사용 594
정책 세부 정보 594
정책 버전 594
JSON 정책 문서 594
자세히 알아보기 595
AmazonKinesisVideoStreamsFullAccess 595
이 정책 사용 595
정책 세부 정보 595
정책 버전 595
JSON 정책 문서 596
자세히 알아보기 596
AmazonKinesisVideoStreamsReadOnlyAccess 596
이 정책 사용 596
정책 세부 정보 596
정책 버전 597
JSON 정책 문서 597
자세히 알아보기 597
AmazonLaunchWizard_Fullaccess 597
이 정책 사용 598
정책 세부 정보 598
정책 버전 598
JSON 정책 문서 598
자세히 알아보기 612

AmazonLaunchWizardFullAccessV2 612
이 정책 사용 613
정책 세부 정보 613
정책 버전 613
JSON 정책 문서 613
자세히 알아보기 630
AmazonLexChannelsAccess 630
이 정책 사용 630
정책 세부 정보 630
정책 버전 630
JSON 정책 문서 630
자세히 알아보기 631
AmazonLexFullAccess 631
이 정책 사용 631
정책 세부 정보 631
정책 버전 631
JSON 정책 문서 632
자세히 알아보기 637
AmazonLexReadOnly 637
이 정책 사용 637
정책 세부 정보 638
정책 버전 638
JSON 정책 문서 638
자세히 알아보기 639
AmazonLexReplicationPolicy 640
이 정책 사용 640
정책 세부 정보 640
정책 버전 640
JSON 정책 문서 640
자세히 알아보기 642
AmazonLexRunBotsOnly 643
이 정책 사용 643
정책 세부 정보 643
정책 버전 643
JSON 정책 문서 643
자세히 알아보기 644

AmazonLexV2BotPolicy 644
이 정책 사용 644
정책 세부 정보 644
정책 버전 644
JSON 정책 문서 645
자세히 알아보기 645
AmazonLookoutEquipmentFullAccess 645
이 정책 사용 645
정책 세부 정보 645
정책 버전 646
JSON 정책 문서 646
자세히 알아보기 647
AmazonLookoutEquipmentReadOnlyAccess 647
이 정책 사용 647
정책 세부 정보 647
정책 버전 648
JSON 정책 문서 648
자세히 알아보기 648
AmazonLookoutMetricsFullAccess 648
이 정책 사용 648
정책 세부 정보 649
정책 버전 649
JSON 정책 문서 649
자세히 알아보기 650
AmazonLookoutMetricsReadOnlyAccess 650
이 정책 사용 650
정책 세부 정보 650
정책 버전 650
JSON 정책 문서 650
자세히 알아보기 651
AmazonLookoutVisionConsoleFullAccess 651
이 정책 사용 651
정책 세부 정보 652
정책 버전 652
JSON 정책 문서 652
자세히 알아보기 654

AmazonLookoutVisionConsoleReadOnlyAccess 654
이 정책 사용 655
정책 세부 정보 655
정책 버전 655
JSON 정책 문서 655
자세히 알아보기 656
AmazonLookoutVisionFullAccess 657
이 정책 사용 657
정책 세부 정보 657
정책 버전 657
JSON 정책 문서 657
자세히 알아보기 658
AmazonLookoutVisionReadOnlyAccess 658
이 정책 사용 658
정책 세부 정보 658
정책 버전 658
JSON 정책 문서 658
자세히 알아보기 659
AmazonMachineLearningBatchPredictionsAccess 659
이 정책 사용 659
정책 세부 정보 659
정책 버전 660
JSON 정책 문서 660
자세히 알아보기 660
AmazonMachineLearningCreateOnlyAccess 661
이 정책 사용 661
정책 세부 정보 661
정책 버전 661
JSON 정책 문서 661
자세히 알아보기 662
AmazonMachineLearningFullAccess 662
이 정책 사용 662
정책 세부 정보 662
정책 버전 662
JSON 정책 문서 662
자세히 알아보기 663

AmazonMachineLearningManageRealTimeEndpointOnlyAccess 663
이 정책 사용 663
정책 세부 정보 663
정책 버전 664
JSON 정책 문서 664
자세히 알아보기 664
AmazonMachineLearningReadOnlyAccess 664
이 정책 사용 664
정책 세부 정보 665
정책 버전 665
JSON 정책 문서 665
자세히 알아보기 665
AmazonMachineLearningRealTimePredictionOnlyAccess 666
이 정책 사용 666
정책 세부 정보 666
정책 버전 666
JSON 정책 문서 666
자세히 알아보기 667
AmazonMachineLearningRoleforRedshiftDataSourceV3 667
이 정책 사용 667
정책 세부 정보 667
정책 버전 667
JSON 정책 문서 668
자세히 알아보기 668
AmazonMacieFullAccess 669
이 정책 사용 669
정책 세부 정보 669
정책 버전 669
JSON 정책 문서 669
자세히 알아보기 670
AmazonMacieHandshakeRole 670
이 정책 사용 670
정책 세부 정보 670
정책 버전 671
JSON 정책 문서 671
자세히 알아보기 671

AmazonMacieReadOnlyAccess 672
이 정책 사용 672
정책 세부 정보 672
정책 버전 672
JSON 정책 문서 672
자세히 알아보기 673
AmazonMacieServiceRole 673
이 정책 사용 673
정책 세부 정보 673
정책 버전 673
JSON 정책 문서 674
자세히 알아보기 674
AmazonMacieServiceRolePolicy 674
이 정책 사용 674
정책 세부 정보 674
정책 버전 675
JSON 정책 문서 675
자세히 알아보기 676
AmazonManagedBlockchainConsoleFullAccess 676
이 정책 사용 676
정책 세부 정보 676
정책 버전 677
JSON 정책 문서 677
자세히 알아보기 677
AmazonManagedBlockchainFullAccess 678
이 정책 사용 678
정책 세부 정보 678
정책 버전 678
JSON 정책 문서 678
자세히 알아보기 679
AmazonManagedBlockchainReadOnlyAccess 679
이 정책 사용 679
정책 세부 정보 679
정책 버전 679
JSON 정책 문서 680
자세히 알아보기 680

AmazonManagedBlockchainServiceRolePolicy 680
이 정책 사용 680
정책 세부 정보 680
정책 버전 681
JSON 정책 문서 681
자세히 알아보기 681
AmazonMCSFullAccess 682
이 정책 사용 682
정책 세부 정보 682
정책 버전 682
JSON 정책 문서 682
자세히 알아보기 683
AmazonMCSReadOnlyAccess 684
이 정책 사용 684
정책 세부 정보 684
정책 버전 684
JSON 정책 문서 684
자세히 알아보기 685
AmazonMechanicalTurkFullAccess 685
이 정책 사용 685
정책 세부 정보 685
정책 버전 686
JSON 정책 문서 686
자세히 알아보기 686
AmazonMechanicalTurkReadOnly 686
이 정책 사용 687
정책 세부 정보 687
정책 버전 687
JSON 정책 문서 687
자세히 알아보기 688
AmazonMemoryDBFullAccess 688
이 정책 사용 688
정책 세부 정보 688
정책 버전 688
JSON 정책 문서 688
자세히 알아보기 689

AmazonMemoryDBReadOnlyAccess 689
이 정책 사용 689
정책 세부 정보 689
정책 버전 690
JSON 정책 문서 690
자세히 알아보기 690
AmazonMobileAnalyticsFinancialReportAccess 690
이 정책 사용 691
정책 세부 정보 691
정책 버전 691
JSON 정책 문서 691
자세히 알아보기 691
AmazonMobileAnalyticsFullAccess 692
이 정책 사용 692
정책 세부 정보 692
정책 버전 692
JSON 정책 문서 692
자세히 알아보기 693
AmazonMobileAnalyticsNon-financialReportAccess 693
이 정책 사용 693
정책 세부 정보 693
정책 버전 693
JSON 정책 문서 694
자세히 알아보기 694
AmazonMobileAnalyticsWriteOnlyAccess 694
이 정책 사용 694
정책 세부 정보 694
정책 버전 695
JSON 정책 문서 695
자세히 알아보기 695
AmazonMonitronFullAccess 695
이 정책 사용 695
정책 세부 정보 696
정책 버전 696
JSON 정책 문서 696
자세히 알아보기 698

AmazonMQApiFullAccess 698
이 정책 사용 698
정책 세부 정보 698
정책 버전 698
JSON 정책 문서 699
자세히 알아보기 700
AmazonMQApiReadOnlyAccess 700
이 정책 사용 700
정책 세부 정보 700
정책 버전 700
JSON 정책 문서 701
자세히 알아보기 701
AmazonMQFullAccess 701
이 정책 사용 701
정책 세부 정보 701
정책 버전 702
JSON 정책 문서 702
자세히 알아보기 703
AmazonMQReadOnlyAccess 703
이 정책 사용 703
정책 세부 정보 703
정책 버전 704
JSON 정책 문서 704
자세히 알아보기 704
AmazonMQServiceRolePolicy 705
이 정책 사용 705
정책 세부 정보 705
정책 버전 705
JSON 정책 문서 705
자세히 알아보기 707
AmazonMSKConnectReadOnlyAccess 707
이 정책 사용 707
정책 세부 정보 707
정책 버전 708
JSON 정책 문서 708
자세히 알아보기 709

AmazonMSKFullAccess 709
이 정책 사용 709
정책 세부 정보 709
정책 버전 709
JSON 정책 문서 710
자세히 알아보기 712
AmazonMSKReadOnlyAccess 713
이 정책 사용 713
정책 세부 정보 713
정책 버전 713
JSON 정책 문서 713
자세히 알아보기 714
AmazonMWAAServiceRolePolicy 714
이 정책 사용 714
정책 세부 정보 714
정책 버전 714
JSON 정책 문서 715
자세히 알아보기 717
AmazonNimbleStudio-LaunchProfileWorker 717
이 정책 사용 717
정책 세부 정보 717
정책 버전 717
JSON 정책 문서 718
자세히 알아보기 718
AmazonNimbleStudio-StudioAdmin 719
이 정책 사용 719
정책 세부 정보 719
정책 버전 719
JSON 정책 문서 719
자세히 알아보기 721
AmazonNimbleStudio-StudioUser 721
이 정책 사용 721
정책 세부 정보 721
정책 버전 722
JSON 정책 문서 722
자세히 알아보기 724

AmazonOmicsFullAccess 724
이 정책 사용 724
정책 세부 정보 724
정책 버전 725
JSON 정책 문서 725
자세히 알아보기 726
AmazonOmicsReadOnlyAccess 726
이 정책 사용 726
정책 세부 정보 726
정책 버전 726
JSON 정책 문서 726
자세히 알아보기 727
AmazonOneEnterpriseFullAccess 727
이 정책 사용 727
정책 세부 정보 727
정책 버전 728
JSON 정책 문서 728
자세히 알아보기 728
AmazonOneEnterpriseInstallerAccess 728
이 정책 사용 728
정책 세부 정보 729
정책 버전 729
JSON 정책 문서 729
자세히 알아보기 729
AmazonOneEnterpriseReadOnlyAccess 730
이 정책 사용 730
정책 세부 정보 730
정책 버전 730
JSON 정책 문서 730
자세히 알아보기 731
AmazonOpenSearchDashboardsServiceRolePolicy 731
이 정책 사용 731
정책 세부 정보 731
정책 버전 731
JSON 정책 문서 732
자세히 알아보기 732

AmazonOpenSearchIngestionFullAccess 732
이 정책 사용 732
정책 세부 정보 732
정책 버전 733
JSON 정책 문서 733
자세히 알아보기 734
AmazonOpenSearchIngestionReadOnlyAccess 734
이 정책 사용 734
정책 세부 정보 734
정책 버전 734
JSON 정책 문서 735
자세히 알아보기 735
AmazonOpenSearchIngestionServiceRolePolicy 735
이 정책 사용 736
정책 세부 정보 736
정책 버전 736
JSON 정책 문서 736
자세히 알아보기 738
AmazonOpenSearchServerlessServiceRolePolicy 738
이 정책 사용 738
정책 세부 정보 738
정책 버전 739
JSON 정책 문서 739
자세히 알아보기 739
AmazonOpenSearchServiceCognitoAccess 739
이 정책 사용 739
정책 세부 정보 740
정책 버전 740
JSON 정책 문서 740
자세히 알아보기 741
AmazonOpenSearchServiceFullAccess 741
이 정책 사용 741
정책 세부 정보 741
정책 버전 742
JSON 정책 문서 742
자세히 알아보기 742

AmazonOpenSearchServiceReadOnlyAccess 742
이 정책 사용 743
정책 세부 정보 743
정책 버전 743
JSON 정책 문서 743
자세히 알아보기 743
AmazonOpenSearchServiceRolePolicy 744
이 정책 사용 744
정책 세부 정보 744
정책 버전 744
JSON 정책 문서 744
자세히 알아보기 749
AmazonPersonalizeFullAccess 749
이 정책 사용 749
정책 세부 정보 749
정책 버전 749
JSON 정책 문서 750
자세히 알아보기 751
AmazonPollyFullAccess 751
이 정책 사용 751
정책 세부 정보 751
정책 버전 751
JSON 정책 문서 752
자세히 알아보기 752
AmazonPollyReadOnlyAccess 752
이 정책 사용 752
정책 세부 정보 753
정책 버전 753
JSON 정책 문서 753
자세히 알아보기 753
AmazonPrometheusConsoleFullAccess 754
이 정책 사용 754
정책 세부 정보 754
정책 버전 754
JSON 정책 문서 754
자세히 알아보기 755

AmazonPrometheusFullAccess 756
이 정책 사용 756
정책 세부 정보 756
정책 버전 756
JSON 정책 문서 756
자세히 알아보기 757
AmazonPrometheusQueryAccess 757
이 정책 사용 758
정책 세부 정보 758
정책 버전 758
JSON 정책 문서 758
자세히 알아보기 759
AmazonPrometheusRemoteWriteAccess 759
이 정책 사용 759
정책 세부 정보 759
정책 버전 759
JSON 정책 문서 759
자세히 알아보기 760
AmazonPrometheusScraperServiceRolePolicy 760
이 정책 사용 760
정책 세부 정보 760
정책 버전 760
JSON 정책 문서 761
자세히 알아보기 763
AmazonQFullAccess 763
이 정책 사용 763
정책 세부 정보 763
정책 버전 763
JSON 정책 문서 763
자세히 알아보기 764
AmazonQLDBConsoleFullAccess 764
이 정책 사용 764
정책 세부 정보 764
정책 버전 764
JSON 정책 문서 765
자세히 알아보기 766

AmazonQLDBFullAccess 767
이 정책 사용 767
정책 세부 정보 767
정책 버전 767
JSON 정책 문서 767
자세히 알아보기 768
AmazonQLDBReadOnly 769
이 정책 사용 769
정책 세부 정보 769
정책 버전 769
JSON 정책 문서 769
자세히 알아보기 770
AmazonRDSBetaServiceRolePolicy 770
이 정책 사용 770
정책 세부 정보 770
정책 버전 771
JSON 정책 문서 771
자세히 알아보기 774
AmazonRDSCustomInstanceProfileRolePolicy 774
이 정책 사용 774
정책 세부 정보 774
정책 버전 775
JSON 정책 문서 775
자세히 알아보기 782
AmazonRDSCustomPreviewServiceRolePolicy 782
이 정책 사용 782
정책 세부 정보 782
정책 버전 783
JSON 정책 문서 783
자세히 알아보기 798
AmazonRDSCustomServiceRolePolicy 798
이 정책 사용 799
정책 세부 정보 799
정책 버전 799
JSON 정책 문서 799
자세히 알아보기 816

AmazonRDSDataFullAccess 816
이 정책 사용 816
정책 세부 정보 816
정책 버전 816
JSON 정책 문서 817
자세히 알아보기 818
AmazonRDSDirectoryServiceAccess 818
이 정책 사용 818
정책 세부 정보 818
정책 버전 818
JSON 정책 문서 819
자세히 알아보기 819
AmazonRDSEnhancedMonitoringRole 819
이 정책 사용 819
정책 세부 정보 820
정책 버전 820
JSON 정책 문서 820
자세히 알아보기 821
AmazonRDSFullAccess 821
이 정책 사용 821
정책 세부 정보 821
정책 버전 821
JSON 정책 문서 822
자세히 알아보기 824
AmazonRDSPerformanceInsightsFullAccess 824
이 정책 사용 824
정책 세부 정보 824
정책 버전 824
JSON 정책 문서 824
자세히 알아보기 826
AmazonRDSPerformanceInsightsReadOnly 826
이 정책 사용 826
정책 세부 정보 826
정책 버전 826
JSON 정책 문서 827
자세히 알아보기 828

AmazonRDSPreviewServiceRolePolicy 829
이 정책 사용 829
정책 세부 정보 829
정책 버전 829
JSON 정책 문서 829
자세히 알아보기 832
AmazonRDSReadOnlyAccess 833
이 정책 사용 833
정책 세부 정보 833
정책 버전 833
JSON 정책 문서 833
자세히 알아보기 834
AmazonRDSServiceRolePolicy 835
이 정책 사용 835
정책 세부 정보 835
정책 버전 835
JSON 정책 문서 835
자세히 알아보기 839
AmazonRedshiftAllCommandsFullAccess 839
이 정책 사용 840
정책 세부 정보 840
정책 버전 840
JSON 정책 문서 840
자세히 알아보기 845
AmazonRedshiftDataFullAccess 846
이 정책 사용 846
정책 세부 정보 846
정책 버전 846
JSON 정책 문서 846
자세히 알아보기 848
AmazonRedshiftFullAccess 848
이 정책 사용 848
정책 세부 정보 849
정책 버전 849
JSON 정책 문서 849
자세히 알아보기 851

AmazonRedshiftQueryEditor 851
이 정책 사용 851
정책 세부 정보 851
정책 버전 852
JSON 정책 문서 852
자세히 알아보기 854
AmazonRedshiftQueryEditorV2FullAccess 854
이 정책 사용 854
정책 세부 정보 854
정책 버전 854
JSON 정책 문서 855
자세히 알아보기 856
AmazonRedshiftQueryEditorV2NoSharing 856
이 정책 사용 856
정책 세부 정보 856
정책 버전 857
JSON 정책 문서 857
자세히 알아보기 860
AmazonRedshiftQueryEditorV2ReadSharing 861
이 정책 사용 861
정책 세부 정보 861
정책 버전 861
JSON 정책 문서 861
자세히 알아보기 866
AmazonRedshiftQueryEditorV2ReadWriteSharing 866
이 정책 사용 867
정책 세부 정보 867
정책 버전 867
JSON 정책 문서 867
자세히 알아보기 872
AmazonRedshiftReadOnlyAccess 872
이 정책 사용 872
정책 세부 정보 872
정책 버전 873
JSON 정책 문서 873
자세히 알아보기 874

AmazonRedshiftServiceLinkedRolePolicy 874
이 정책 사용 874
정책 세부 정보 874
정책 버전 874
JSON 정책 문서 874
자세히 알아보기 880
AmazonRekognitionCustomLabelsFullAccess 880
이 정책 사용 880
정책 세부 정보 880
정책 버전 880
JSON 정책 문서 881
자세히 알아보기 882
AmazonRekognitionFullAccess 882
이 정책 사용 882
정책 세부 정보 882
정책 버전 882
JSON 정책 문서 883
자세히 알아보기 883
AmazonRekognitionReadOnlyAccess 883
이 정책 사용 883
정책 세부 정보 883
정책 버전 884
JSON 정책 문서 884
자세히 알아보기 885
AmazonRekognitionServiceRole 885
이 정책 사용 885
정책 세부 정보 885
정책 버전 886
JSON 정책 문서 886
자세히 알아보기 887
AmazonRoute53AutoNamingFullAccess 887
이 정책 사용 887
정책 세부 정보 887
정책 버전 887
JSON 정책 문서 887
자세히 알아보기 888

AmazonRoute53AutoNamingReadOnlyAccess 888
이 정책 사용 888
정책 세부 정보 889
정책 버전 889
JSON 정책 문서 889
자세히 알아보기 889
AmazonRoute53AutoNamingRegistrantAccess 890
이 정책 사용 890
정책 세부 정보 890
정책 버전 890
JSON 정책 문서 890
자세히 알아보기 891
AmazonRoute53DomainsFullAccess 891
이 정책 사용 891
정책 세부 정보 891
정책 버전 892
JSON 정책 문서 892
자세히 알아보기 892
AmazonRoute53DomainsReadOnlyAccess 892
이 정책 사용 893
정책 세부 정보 893
정책 버전 893
JSON 정책 문서 893
자세히 알아보기 894
AmazonRoute53FullAccess 894
이 정책 사용 894
정책 세부 정보 894
정책 버전 894
JSON 정책 문서 894
자세히 알아보기 895
AmazonRoute53ReadOnlyAccess 895
이 정책 사용 896
정책 세부 정보 896
정책 버전 896
JSON 정책 문서 896
자세히 알아보기 897

AmazonRoute53RecoveryClusterFullAccess 897
이 정책 사용 897
정책 세부 정보 897
정책 버전 897
JSON 정책 문서 897
자세히 알아보기 898
AmazonRoute53RecoveryClusterReadOnlyAccess 898
이 정책 사용 898
정책 세부 정보 898
정책 버전 898
JSON 정책 문서 899
자세히 알아보기 899
AmazonRoute53RecoveryControlConfigFullAccess 899
이 정책 사용 899
정책 세부 정보 900
정책 버전 900
JSON 정책 문서 900
자세히 알아보기 900
AmazonRoute53RecoveryControlConfigReadOnlyAccess 901
이 정책 사용 901
정책 세부 정보 901
정책 버전 901
JSON 정책 문서 901
자세히 알아보기 902
AmazonRoute53RecoveryReadinessFullAccess 902
이 정책 사용 902
정책 세부 정보 902
정책 버전 903
JSON 정책 문서 903
자세히 알아보기 903
AmazonRoute53RecoveryReadinessReadOnlyAccess 903
이 정책 사용 903
정책 세부 정보 904
정책 버전 904
JSON 정책 문서 904
자세히 알아보기 905

AmazonRoute53ResolverFullAccess 905
이 정책 사용 905
정책 세부 정보 905
정책 버전 905
JSON 정책 문서 906
자세히 알아보기 906
AmazonRoute53ResolverReadOnlyAccess 907
이 정책 사용 907
정책 세부 정보 907
정책 버전 907
JSON 정책 문서 907
자세히 알아보기 908
AmazonS3FullAccess 908
이 정책 사용 908
정책 세부 정보 908
정책 버전 908
JSON 정책 문서 909
자세히 알아보기 909
AmazonS3ObjectLambdaExecutionRolePolicy 909
이 정책 사용 909
정책 세부 정보 909
정책 버전 910
JSON 정책 문서 910
자세히 알아보기 910
AmazonS3OutpostsFullAccess 911
이 정책 사용 911
정책 세부 정보 911
정책 버전 911
JSON 정책 문서 911
자세히 알아보기 912
AmazonS3OutpostsReadOnlyAccess 912
이 정책 사용 912
정책 세부 정보 913
정책 버전 913
JSON 정책 문서 913
자세히 알아보기 914

AmazonS3ReadOnlyAccess 914
이 정책 사용 914
정책 세부 정보 914
정책 버전 915
JSON 정책 문서 915
자세히 알아보기 915
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 916
이 정책 사용 916
정책 세부 정보 916
정책 버전 916
JSON 정책 문서 916
자세히 알아보기 926
AmazonSageMakerCanvasAIServicesAccess 927
이 정책 사용 927
정책 세부 정보 927
정책 버전 927
JSON 정책 문서 927
자세히 알아보기 930
AmazonSageMakerCanvasBedrockAccess 931
이 정책 사용 931
정책 세부 정보 931
정책 버전 931
JSON 정책 문서 931
자세히 알아보기 932
AmazonSageMakerCanvasDataPrepFullAccess 932
이 정책 사용 932
정책 세부 정보 932
정책 버전 933
JSON 정책 문서 933
자세히 알아보기 940
AmazonSageMakerCanvasDirectDeployAccess 940
이 정책 사용 940
정책 세부 정보 940
정책 버전 941
JSON 정책 문서 941
자세히 알아보기 941

AmazonSageMakerCanvasForecastAccess 942
이 정책 사용 942
정책 세부 정보 942
정책 버전 942
JSON 정책 문서 942
자세히 알아보기 943
AmazonSageMakerCanvasFullAccess 943
이 정책 사용 943
정책 세부 정보 943
정책 버전 944
JSON 정책 문서 944
자세히 알아보기 952
AmazonSageMakerClusterInstanceRolePolicy 952
이 정책 사용 952
정책 세부 정보 952
정책 버전 952
JSON 정책 문서 953
자세히 알아보기 954
AmazonSageMakerCoreServiceRolePolicy 955
이 정책 사용 955
정책 세부 정보 955
정책 버전 955
JSON 정책 문서 955
자세히 알아보기 956
AmazonSageMakerEdgeDeviceFleetPolicy 956
이 정책 사용 956
정책 세부 정보 957
정책 버전 957
JSON 정책 문서 957
자세히 알아보기 959
AmazonSageMakerFeatureStoreAccess 959
이 정책 사용 959
정책 세부 정보 959
정책 버전 959
JSON 정책 문서 960
자세히 알아보기 961

AmazonSageMakerFullAccess 961
이 정책 사용 961
정책 세부 정보 961
정책 버전 961
JSON 정책 문서 962
자세히 알아보기 977
AmazonSageMakerGeospatialExecutionRole 977
이 정책 사용 978
정책 세부 정보 978
정책 버전 978
JSON 정책 문서 978
자세히 알아보기 979
AmazonSageMakerGeospatialFullAccess 979
이 정책 사용 979
정책 세부 정보 979
정책 버전 980
JSON 정책 문서 980
자세히 알아보기 980
AmazonSageMakerGroundTruthExecution 981
이 정책 사용 981
정책 세부 정보 981
정책 버전 981
JSON 정책 문서 981
자세히 알아보기 985
AmazonSageMakerMechanicalTurkAccess 985
이 정책 사용 985
정책 세부 정보 985
정책 버전 985
JSON 정책 문서 985
자세히 알아보기 986
AmazonSageMakerModelGovernanceUseAccess 986
이 정책 사용 986
정책 세부 정보 986
정책 버전 987
JSON 정책 문서 987
자세히 알아보기 988

AmazonSageMakerModelRegistryFullAccess 989
이 정책 사용 989
정책 세부 정보 989
정책 버전 989
JSON 정책 문서 989
자세히 알아보기 992
AmazonSageMakerNotebooksServiceRolePolicy 992
이 정책 사용 993
정책 세부 정보 993
정책 버전 993
JSON 정책 문서 993
자세히 알아보기 996
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 996
이 정책 사용 997
정책 세부 정보 997
정책 버전 997
JSON 정책 문서 997
자세히 알아보기 998
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 998
이 정책 사용 998
정책 세부 정보 999
정책 버전 999
JSON 정책 문서 999
자세히 알아보기 1002
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1003
이 정책 사용 1003
정책 세부 정보 1003
정책 버전 1003
JSON 정책 문서 1003
자세히 알아보기 1004
AmazonSageMakerPipelinesIntegrations 1004
이 정책 사용 1004
정책 세부 정보 1004
정책 버전 1005
JSON 정책 문서 1005
자세히 알아보기 1007

AmazonSageMakerReadOnly 1007
이 정책 사용 1007
정책 세부 정보 1007
정책 버전 1007
JSON 정책 문서 1007
자세히 알아보기 1009
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1009
이 정책 사용 1009
정책 세부 정보 1009
정책 버전 1009
JSON 정책 문서 1010
자세히 알아보기 1010
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1011
이 정책 사용 1011
정책 세부 정보 1011
정책 버전 1011
JSON 정책 문서 1011
자세히 알아보기 1018
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1018
이 정책 사용 1019
정책 세부 정보 1019
정책 버전 1019
JSON 정책 문서 1019
자세히 알아보기 1028
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1029
이 정책 사용 1029
정책 세부 정보 1029
정책 버전 1029
JSON 정책 문서 1029
자세히 알아보기 1031
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1031
이 정책 사용 1031
정책 세부 정보 1031
정책 버전 1032
JSON 정책 문서 1032
자세히 알아보기 1032

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1032
이 정책 사용 1033
정책 세부 정보 1033
정책 버전 1033
JSON 정책 문서 1033
자세히 알아보기 1034
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1034
이 정책 사용 1034
정책 세부 정보 1034
정책 버전 1034
JSON 정책 문서 1035
자세히 알아보기 1037
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1037
이 정책 사용 1037
정책 세부 정보 1037
정책 버전 1037
JSON 정책 문서 1038
자세히 알아보기 1047
AmazonSecurityLakeAdministrator 1047
이 정책 사용 1048
정책 세부 정보 1048
정책 버전 1048
JSON 정책 문서 1048
자세히 알아보기 1059
AmazonSecurityLakeMetastoreManager 1059
이 정책 사용 1060
정책 세부 정보 1060
정책 버전 1060
JSON 정책 문서 1060
자세히 알아보기 1062
AmazonSecurityLakePermissionsBoundary 1062
이 정책 사용 1062
정책 세부 정보 1062
정책 버전 1063
JSON 정책 문서 1063
자세히 알아보기 1066

AmazonSESFullAccess 1066
이 정책 사용 1066
정책 세부 정보 1066
정책 버전 1066
JSON 정책 문서 1067
자세히 알아보기 1067
AmazonSESReadOnlyAccess 1067
이 정책 사용 1067
정책 세부 정보 1067
정책 버전 1068
JSON 정책 문서 1068
자세히 알아보기 1068
AmazonSNSFullAccess 1068
이 정책 사용 1069
정책 세부 정보 1069
정책 버전 1069
JSON 정책 문서 1069
자세히 알아보기 1069
AmazonSNSReadOnlyAccess 1070
이 정책 사용 1070
정책 세부 정보 1070
정책 버전 1070
JSON 정책 문서 1070
자세히 알아보기 1071
AmazonSNSRole 1071
이 정책 사용 1071
정책 세부 정보 1071
정책 버전 1071
JSON 정책 문서 1071
자세히 알아보기 1072
AmazonSQSFullAccess 1072
이 정책 사용 1072
정책 세부 정보 1072
정책 버전 1073
JSON 정책 문서 1073
자세히 알아보기 1073

AmazonSQSReadOnlyAccess 1073
이 정책 사용 1073
정책 세부 정보 1074
정책 버전 1074
JSON 정책 문서 1074
자세히 알아보기 1074
AmazonSSMAutomationApproverAccess 1075
이 정책 사용 1075
정책 세부 정보 1075
정책 버전 1075
JSON 정책 문서 1075
자세히 알아보기 1076
AmazonSSMAutomationRole 1076
이 정책 사용 1076
정책 세부 정보 1076
정책 버전 1076
JSON 정책 문서 1077
자세히 알아보기 1078
AmazonSSMDirectoryServiceAccess 1078
이 정책 사용 1078
정책 세부 정보 1079
정책 버전 1079
JSON 정책 문서 1079
자세히 알아보기 1079
AmazonSSMFullAccess 1080
이 정책 사용 1080
정책 세부 정보 1080
정책 버전 1080
JSON 정책 문서 1080
자세히 알아보기 1081
AmazonSSMMaintenanceWindowRole 1082
이 정책 사용 1082
정책 세부 정보 1082
정책 버전 1082
JSON 정책 문서 1082
자세히 알아보기 1084

AmazonSSMManagedEC2InstanceDefaultPolicy 1084
이 정책 사용 1084
정책 세부 정보 1084
정책 버전 1084
JSON 정책 문서 1084
자세히 알아보기 1086
AmazonSSMManagedInstanceCore 1086
이 정책 사용 1086
정책 세부 정보 1086
정책 버전 1086
JSON 정책 문서 1086
자세히 알아보기 1088
AmazonSSMPatchAssociation 1088
이 정책 사용 1088
정책 세부 정보 1088
정책 버전 1088
JSON 정책 문서 1088
자세히 알아보기 1089
AmazonSSMReadOnlyAccess 1089
이 정책 사용 1089
정책 세부 정보 1090
정책 버전 1090
JSON 정책 문서 1090
자세히 알아보기 1090
AmazonSSMServiceRolePolicy 1091
이 정책 사용 1091
정책 세부 정보 1091
정책 버전 1091
JSON 정책 문서 1091
자세히 알아보기 1096
AmazonSumerianFullAccess 1096
이 정책 사용 1097
정책 세부 정보 1097
정책 버전 1097
JSON 정책 문서 1097
자세히 알아보기 1097

AmazonTextractFullAccess 1098
이 정책 사용 1098
정책 세부 정보 1098
정책 버전 1098
JSON 정책 문서 1098
자세히 알아보기 1099
AmazonTextractServiceRole 1099
이 정책 사용 1099
정책 세부 정보 1099
정책 버전 1099
JSON 정책 문서 1100
자세히 알아보기 1100
AmazonTimestreamConsoleFullAccess 1100
이 정책 사용 1100
정책 세부 정보 1100
정책 버전 1101
JSON 정책 문서 1101
자세히 알아보기 1102
AmazonTimestreamFullAccess 1103
이 정책 사용 1103
정책 세부 정보 1103
정책 버전 1103
JSON 정책 문서 1103
자세히 알아보기 1104
AmazonTimestreamInfluxDBFullAccess 1105
이 정책 사용 1105
정책 세부 정보 1105
정책 버전 1105
JSON 정책 문서 1105
자세히 알아보기 1107
AmazonTimestreamInfluxDBServiceRolePolicy 1107
이 정책 사용 1108
정책 세부 정보 1108
정책 버전 1108
JSON 정책 문서 1108
자세히 알아보기 1111

AmazonTimestreamReadOnlyAccess 1111
이 정책 사용 1111
정책 세부 정보 1111
정책 버전 1111
JSON 정책 문서 1111
자세히 알아보기 1112
AmazonTranscribeFullAccess 1112
이 정책 사용 1112
정책 세부 정보 1113
정책 버전 1113
JSON 정책 문서 1113
자세히 알아보기 1114
AmazonTranscribeReadOnlyAccess 1114
이 정책 사용 1114
정책 세부 정보 1114
정책 버전 1114
JSON 정책 문서 1114
자세히 알아보기 1115
AmazonVPCCrossAccountNetworkInterfaceOperations 1115
이 정책 사용 1115
정책 세부 정보 1115
정책 버전 1116
JSON 정책 문서 1116
자세히 알아보기 1117
AmazonVPCFullAccess 1117
이 정책 사용 1117
정책 세부 정보 1118
정책 버전 1118
JSON 정책 문서 1118
자세히 알아보기 1122
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1122
이 정책 사용 1122
정책 세부 정보 1122
정책 버전 1123
JSON 정책 문서 1123
자세히 알아보기 1126

AmazonVPCReachabilityAnalyzerFullAccessPolicy 1126
이 정책 사용 1126
정책 세부 정보 1126
정책 버전 1127
JSON 정책 문서 1127
자세히 알아보기 1130
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1130
이 정책 사용 1130
정책 세부 정보 1130
정책 버전 1130
JSON 정책 문서 1131
자세히 알아보기 1131
AmazonVPCReadOnlyAccess 1131
이 정책 사용 1131
정책 세부 정보 1131
정책 버전 1132
JSON 정책 문서 1132
자세히 알아보기 1133
AmazonWorkDocsFullAccess 1133
이 정책 사용 1133
정책 세부 정보 1134
정책 버전 1134
JSON 정책 문서 1134
자세히 알아보기 1134
AmazonWorkDocsReadOnlyAccess 1135
이 정책 사용 1135
정책 세부 정보 1135
정책 버전 1135
JSON 정책 문서 1135
자세히 알아보기 1136
AmazonWorkMailEventsServiceRolePolicy 1136
이 정책 사용 1136
정책 세부 정보 1136
정책 버전 1136
JSON 정책 문서 1137
자세히 알아보기 1137

AmazonWorkMailFullAccess 1137
이 정책 사용 1137
정책 세부 정보 1137
정책 버전 1138
JSON 정책 문서 1138
자세히 알아보기 1140
AmazonWorkMailMessageFlowFullAccess 1140
이 정책 사용 1140
정책 세부 정보 1140
정책 버전 1140
JSON 정책 문서 1141
자세히 알아보기 1141
AmazonWorkMailMessageFlowReadOnlyAccess 1141
이 정책 사용 1141
정책 세부 정보 1141
정책 버전 1142
JSON 정책 문서 1142
자세히 알아보기 1142
AmazonWorkMailReadOnlyAccess 1142
이 정책 사용 1142
정책 세부 정보 1143
정책 버전 1143
JSON 정책 문서 1143
자세히 알아보기 1144
AmazonWorkSpacesAdmin 1144
이 정책 사용 1144
정책 세부 정보 1144
정책 버전 1144
JSON 정책 문서 1144
자세히 알아보기 1145
AmazonWorkSpacesApplicationManagerAdminAccess 1146
이 정책 사용 1146
정책 세부 정보 1146
정책 버전 1146
JSON 정책 문서 1146
자세히 알아보기 1147

AmazonWorkspacesPCAAccess 1147
이 정책 사용 1147
정책 세부 정보 1147
정책 버전 1147
JSON 정책 문서 1147
자세히 알아보기 1148
AmazonWorkSpacesSelfServiceAccess 1148
이 정책 사용 1148
정책 세부 정보 1148
정책 버전 1149
JSON 정책 문서 1149
자세히 알아보기 1149
AmazonWorkSpacesServiceAccess 1149
이 정책 사용 1150
정책 세부 정보 1150
정책 버전 1150
JSON 정책 문서 1150
자세히 알아보기 1150
AmazonWorkSpacesWebReadOnly 1151
이 정책 사용 1151
정책 세부 정보 1151
정책 버전 1151
JSON 정책 문서 1151
자세히 알아보기 1152
AmazonWorkSpacesWebServiceRolePolicy 1153
이 정책 사용 1153
정책 세부 정보 1153
정책 버전 1153
JSON 정책 문서 1153
자세히 알아보기 1156
AmazonZocaloFullAccess 1156
이 정책 사용 1156
정책 세부 정보 1156
정책 버전 1156
JSON 정책 문서 1156
자세히 알아보기 1157

AmazonZocaloReadOnlyAccess 1157
이 정책 사용 1157
정책 세부 정보 1158
정책 버전 1158
JSON 정책 문서 1158
자세히 알아보기 1158
AmplifyBackendDeployFullAccess 1159
이 정책 사용 1159
정책 세부 정보 1159
정책 버전 1159
JSON 정책 문서 1159
자세히 알아보기 1162
APIGatewayServiceRolePolicy 1163
이 정책 사용 1163
정책 세부 정보 1163
정책 버전 1163
JSON 정책 문서 1163
자세히 알아보기 1165
AppIntegrationsServiceLinkedRolePolicy 1166
이 정책 사용 1166
정책 세부 정보 1166
정책 버전 1166
JSON 정책 문서 1166
자세히 알아보기 1168
ApplicationAutoScalingForAmazonAppStreamAccess 1168
이 정책 사용 1168
정책 세부 정보 1168
정책 버전 1168
JSON 정책 문서 1169
자세히 알아보기 1169
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1170
이 정책 사용 1170
정책 세부 정보 1170
정책 버전 1170
JSON 정책 문서 1170
자세히 알아보기 1172

AppRunnerNetworkingServiceRolePolicy 1172
이 정책 사용 1172
정책 세부 정보 1173
정책 버전 1173
JSON 정책 문서 1173
자세히 알아보기 1174
AppRunnerServiceRolePolicy 1174
이 정책 사용 1175
정책 세부 정보 1175
정책 버전 1175
JSON 정책 문서 1175
자세히 알아보기 1176
AutoScalingConsoleFullAccess 1176
이 정책 사용 1176
정책 세부 정보 1176
정책 버전 1177
JSON 정책 문서 1177
자세히 알아보기 1178
AutoScalingConsoleReadOnlyAccess 1179
이 정책 사용 1179
정책 세부 정보 1179
정책 버전 1179
JSON 정책 문서 1179
자세히 알아보기 1180
AutoScalingFullAccess 1181
이 정책 사용 1181
정책 세부 정보 1181
정책 버전 1181
JSON 정책 문서 1181
자세히 알아보기 1182
AutoScalingNotificationAccessRole 1183
이 정책 사용 1183
정책 세부 정보 1183
정책 버전 1183
JSON 정책 문서 1183
자세히 알아보기 1184

AutoScalingReadOnlyAccess 1184
이 정책 사용 1184
정책 세부 정보 1184
정책 버전 1184
JSON 정책 문서 1185
자세히 알아보기 1185
AutoScalingServiceRolePolicy 1185
이 정책 사용 1185
정책 세부 정보 1185
정책 버전 1186
JSON 정책 문서 1186
자세히 알아보기 1189
AWS_ConfigRole 1189
이 정책 사용 1189
정책 세부 정보 1189
정책 버전 1189
JSON 정책 문서 1189
자세히 알아보기 1220
AWSAccountActivityAccess 1220
이 정책 사용 1220
정책 세부 정보 1220
정책 버전 1221
JSON 정책 문서 1221
자세히 알아보기 1222
AWSAccountManagementFullAccess 1222
이 정책 사용 1222
정책 세부 정보 1222
정책 버전 1222
JSON 정책 문서 1222
자세히 알아보기 1223
AWSAccountManagementReadOnlyAccess 1223
이 정책 사용 1223
정책 세부 정보 1223
정책 버전 1223
JSON 정책 문서 1224
자세히 알아보기 1224

AWSAccountUsageReportAccess 1224
이 정책 사용 1224
정책 세부 정보 1224
정책 버전 1225
JSON 정책 문서 1225
자세히 알아보기 1225
AWSAgentlessDiscoveryService 1225
이 정책 사용 1225
정책 세부 정보 1226
정책 버전 1226
JSON 정책 문서 1226
자세히 알아보기 1228
AWSAppFabricFullAccess 1228
이 정책 사용 1228
정책 세부 정보 1228
정책 버전 1228
JSON 정책 문서 1229
자세히 알아보기 1230
AWSAppFabricReadOnlyAccess 1230
이 정책 사용 1230
정책 세부 정보 1230
정책 버전 1231
JSON 정책 문서 1231
자세히 알아보기 1231
AWSAppFabricServiceRolePolicy 1232
이 정책 사용 1232
정책 세부 정보 1232
정책 버전 1232
JSON 정책 문서 1232
자세히 알아보기 1233
AWSApplicationAutoscalingAppStreamFleetPolicy 1234
이 정책 사용 1234
정책 세부 정보 1234
정책 버전 1234
JSON 정책 문서 1234
자세히 알아보기 1235

AWSApplicationAutoscalingCassandraTablePolicy 1235
이 정책 사용 1235
정책 세부 정보 1235
정책 버전 1235
JSON 정책 문서 1236
자세히 알아보기 1236
AWSApplicationAutoscalingComprehendEndpointPolicy 1236
이 정책 사용 1237
정책 세부 정보 1237
정책 버전 1237
JSON 정책 문서 1237
자세히 알아보기 1238
AWSApplicationAutoScalingCustomResourcePolicy 1238
이 정책 사용 1238
정책 세부 정보 1238
정책 버전 1238
JSON 정책 문서 1238
자세히 알아보기 1239
AWSApplicationAutoscalingDynamoDBTablePolicy 1239
이 정책 사용 1239
정책 세부 정보 1239
정책 버전 1240
JSON 정책 문서 1240
자세히 알아보기 1240
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1240
이 정책 사용 1241
정책 세부 정보 1241
정책 버전 1241
JSON 정책 문서 1241
자세히 알아보기 1242
AWSApplicationAutoscalingECSServicePolicy 1242
이 정책 사용 1242
정책 세부 정보 1242
정책 버전 1242
JSON 정책 문서 1242
자세히 알아보기 1243

AWSApplicationAutoscalingElastiCacheRGPolicy 1243
이 정책 사용 1243
정책 세부 정보 1243
정책 버전 1244
JSON 정책 문서 1244
자세히 알아보기 1245
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1245
이 정책 사용 1245
정책 세부 정보 1245
정책 버전 1245
JSON 정책 문서 1245
자세히 알아보기 1246
AWSApplicationAutoscalingKafkaClusterPolicy 1246
이 정책 사용 1246
정책 세부 정보 1246
정책 버전 1247
JSON 정책 문서 1247
자세히 알아보기 1247
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1247
이 정책 사용 1248
정책 세부 정보 1248
정책 버전 1248
JSON 정책 문서 1248
자세히 알아보기 1249
AWSApplicationAutoscalingNeptuneClusterPolicy 1249
이 정책 사용 1249
정책 세부 정보 1249
정책 버전 1249
JSON 정책 문서 1250
자세히 알아보기 1251
AWSApplicationAutoscalingRDSClusterPolicy 1251
이 정책 사용 1251
정책 세부 정보 1251
정책 버전 1252
JSON 정책 문서 1252
자세히 알아보기 1253

AWSApplicationAutoscalingSageMakerEndpointPolicy 1253
이 정책 사용 1253
정책 세부 정보 1253
정책 버전 1253
JSON 정책 문서 1254
자세히 알아보기 1254
AWSApplicationDiscoveryAgentAccess 1255
이 정책 사용 1255
정책 세부 정보 1255
정책 버전 1255
JSON 정책 문서 1255
자세히 알아보기 1256
AWSApplicationDiscoveryAgentlessCollectorAccess 1256
이 정책 사용 1256
정책 세부 정보 1256
정책 버전 1256
JSON 정책 문서 1257
자세히 알아보기 1258
AWSApplicationDiscoveryServiceFullAccess 1258
이 정책 사용 1258
정책 세부 정보 1258
정책 버전 1258
JSON 정책 문서 1259
자세히 알아보기 1260
AWSApplicationMigrationAgentInstallationPolicy 1260
이 정책 사용 1260
정책 세부 정보 1260
정책 버전 1261
JSON 정책 문서 1261
자세히 알아보기 1262
AWSApplicationMigrationAgentPolicy 1262
이 정책 사용 1262
정책 세부 정보 1262
정책 버전 1262
JSON 정책 문서 1263
자세히 알아보기 1264

AWSApplicationMigrationAgentPolicy_v2 1264
이 정책 사용 1264
정책 세부 정보 1264
정책 버전 1264
JSON 정책 문서 1264
자세히 알아보기 1265
AWSApplicationMigrationConversionServerPolicy 1265
이 정책 사용 1266
정책 세부 정보 1266
정책 버전 1266
JSON 정책 문서 1266
자세히 알아보기 1267
AWSApplicationMigrationEC2Access 1267
이 정책 사용 1267
정책 세부 정보 1267
정책 버전 1267
JSON 정책 문서 1267
자세히 알아보기 1275
AWSApplicationMigrationFullAccess 1275
이 정책 사용 1275
정책 세부 정보 1276
정책 버전 1276
JSON 정책 문서 1276
자세히 알아보기 1281
AWSApplicationMigrationMGHAccess 1281
이 정책 사용 1282
정책 세부 정보 1282
정책 버전 1282
JSON 정책 문서 1282
자세히 알아보기 1283
AWSApplicationMigrationReadOnlyAccess 1283
이 정책 사용 1283
정책 세부 정보 1283
정책 버전 1283
JSON 정책 문서 1284
자세히 알아보기 1285

AWSApplicationMigrationReplicationServerPolicy 1285
이 정책 사용 1285
정책 세부 정보 1285
정책 버전 1286
JSON 정책 문서 1286
자세히 알아보기 1287
AWSApplicationMigrationServiceEc2InstancePolicy 1288
이 정책 사용 1288
정책 세부 정보 1288
정책 버전 1288
JSON 정책 문서 1288
자세히 알아보기 1289
AWSApplicationMigrationServiceRolePolicy 1290
이 정책 사용 1290
정책 세부 정보 1290
정책 버전 1290
JSON 정책 문서 1290
자세히 알아보기 1297
AWSApplicationMigrationSSMAccess 1297
이 정책 사용 1298
정책 세부 정보 1298
정책 버전 1298
JSON 정책 문서 1298
자세히 알아보기 1300
AWSApplicationMigrationVCenterClientPolicy 1300
이 정책 사용 1300
정책 세부 정보 1300
정책 버전 1301
JSON 정책 문서 1301
자세히 알아보기 1301
AWSAppMeshEnvoyAccess 1302
이 정책 사용 1302
정책 세부 정보 1302
정책 버전 1302
JSON 정책 문서 1302
자세히 알아보기 1303

AWSAppMeshFullAccess 1303
이 정책 사용 1303
정책 세부 정보 1303
정책 버전 1303
JSON 정책 문서 1304
자세히 알아보기 1305
AWSAppMeshPreviewEnvoyAccess 1305
이 정책 사용 1305
정책 세부 정보 1305
정책 버전 1306
JSON 정책 문서 1306
자세히 알아보기 1306
AWSAppMeshPreviewServiceRolePolicy 1306
이 정책 사용 1306
정책 세부 정보 1307
정책 버전 1307
JSON 정책 문서 1307
자세히 알아보기 1308
AWSAppMeshReadOnly 1308
이 정책 사용 1308
정책 세부 정보 1308
정책 버전 1308
JSON 정책 문서 1308
자세히 알아보기 1309
AWSAppMeshServiceRolePolicy 1310
이 정책 사용 1310
정책 세부 정보 1310
정책 버전 1310
JSON 정책 문서 1310
자세히 알아보기 1311
AWSAppRunnerFullAccess 1311
이 정책 사용 1311
정책 세부 정보 1311
정책 버전 1311
JSON 정책 문서 1312
자세히 알아보기 1312

AWSAppRunnerReadOnlyAccess 1313
이 정책 사용 1313
정책 세부 정보 1313
정책 버전 1313
JSON 정책 문서 1313
자세히 알아보기 1314
AWSAppRunnerServicePolicyForECRAccess 1314
이 정책 사용 1314
정책 세부 정보 1314
정책 버전 1314
JSON 정책 문서 1314
자세히 알아보기 1315
AWSAppSyncAdministrator 1315
이 정책 사용 1315
정책 세부 정보 1315
정책 버전 1316
JSON 정책 문서 1316
자세히 알아보기 1317
AWSAppSyncInvokeFullAccess 1317
이 정책 사용 1317
정책 세부 정보 1317
정책 버전 1318
JSON 정책 문서 1318
자세히 알아보기 1318
AWSAppSyncPushToCloudWatchLogs 1318
이 정책 사용 1319
정책 세부 정보 1319
정책 버전 1319
JSON 정책 문서 1319
자세히 알아보기 1319
AWSAppSyncSchemaAuthor 1320
이 정책 사용 1320
정책 세부 정보 1320
정책 버전 1320
JSON 정책 문서 1320
자세히 알아보기 1321

AWSAppSyncServiceRolePolicy 1322
이 정책 사용 1322
정책 세부 정보 1322
정책 버전 1322
JSON 정책 문서 1322
자세히 알아보기 1323
AWSArtifactAccountSync 1323
이 정책 사용 1323
정책 세부 정보 1323
정책 버전 1323
JSON 정책 문서 1324
자세히 알아보기 1324
AWSArtifactReportsReadOnlyAccess 1324
이 정책 사용 1324
정책 세부 정보 1324
정책 버전 1325
JSON 정책 문서 1325
자세히 알아보기 1325
AWSArtifactServiceRolePolicy 1325
이 정책 사용 1326
정책 세부 정보 1326
정책 버전 1326
JSON 정책 문서 1326
자세히 알아보기 1327
AWSAuditManagerAdministratorAccess 1327
이 정책 사용 1327
정책 세부 정보 1327
정책 버전 1327
JSON 정책 문서 1327
자세히 알아보기 1331
AWSAuditManagerServiceRolePolicy 1331
이 정책 사용 1331
정책 세부 정보 1332
정책 버전 1332
JSON 정책 문서 1332
자세히 알아보기 1336

AWSAutoScalingPlansEC2AutoScalingPolicy 1337
이 정책 사용 1337
정책 세부 정보 1337
정책 버전 1337
JSON 정책 문서 1337
자세히 알아보기 1338
AWSBackupAuditAccess 1338
이 정책 사용 1338
정책 세부 정보 1338
정책 버전 1338
JSON 정책 문서 1339
자세히 알아보기 1340
AWSBackupDataTransferAccess 1340
이 정책 사용 1340
정책 세부 정보 1340
정책 버전 1341
JSON 정책 문서 1341
자세히 알아보기 1341
AWSBackupFullAccess 1342
이 정책 사용 1342
정책 세부 정보 1342
정책 버전 1342
JSON 정책 문서 1342
자세히 알아보기 1352
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1352
이 정책 사용 1352
정책 세부 정보 1352
정책 버전 1353
JSON 정책 문서 1353
자세히 알아보기 1353
AWSBackupOperatorAccess 1354
이 정책 사용 1354
정책 세부 정보 1354
정책 버전 1354
JSON 정책 문서 1354
자세히 알아보기 1361

AWSBackupOrganizationAdminAccess 1361
이 정책 사용 1361
정책 세부 정보 1362
정책 버전 1362
JSON 정책 문서 1362
자세히 알아보기 1364
AWSBackupRestoreAccessForSAPHANA 1364
이 정책 사용 1364
정책 세부 정보 1364
정책 버전 1364
JSON 정책 문서 1365
자세히 알아보기 1366
AWSBackupServiceLinkedRolePolicyForBackup 1366
이 정책 사용 1366
정책 세부 정보 1366
정책 버전 1366
JSON 정책 문서 1366
자세히 알아보기 1374
AWSBackupServiceLinkedRolePolicyForBackupTest 1374
이 정책 사용 1374
정책 세부 정보 1374
정책 버전 1375
JSON 정책 문서 1375
자세히 알아보기 1376
AWSBackupServiceRolePolicyForBackup 1376
이 정책 사용 1376
정책 세부 정보 1376
정책 버전 1376
JSON 정책 문서 1376
자세히 알아보기 1387
AWSBackupServiceRolePolicyForRestores 1387
이 정책 사용 1387
정책 세부 정보 1387
정책 버전 1388
JSON 정책 문서 1388
자세히 알아보기 1398

AWSBackupServiceRolePolicyForS3Backup 1398
이 정책 사용 1398
정책 세부 정보 1398
정책 버전 1398
JSON 정책 문서 1399
자세히 알아보기 1400
AWSBackupServiceRolePolicyForS3Restore 1401
이 정책 사용 1401
정책 세부 정보 1401
정책 버전 1401
JSON 정책 문서 1401
자세히 알아보기 1403
AWSBatchFullAccess 1403
이 정책 사용 1403
정책 세부 정보 1403
정책 버전 1403
JSON 정책 문서 1403
자세히 알아보기 1405
AWSBatchServiceEventTargetRole 1405
이 정책 사용 1405
정책 세부 정보 1405
정책 버전 1406
JSON 정책 문서 1406
자세히 알아보기 1406
AWSBatchServiceRole 1406
이 정책 사용 1406
정책 세부 정보 1407
정책 버전 1407
JSON 정책 문서 1407
자세히 알아보기 1410
AWSBillingConductorFullAccess 1410
이 정책 사용 1410
정책 세부 정보 1411
정책 버전 1411
JSON 정책 문서 1411
자세히 알아보기 1411

AWSBillingConductorReadOnlyAccess 1412
이 정책 사용 1412
정책 세부 정보 1412
정책 버전 1412
JSON 정책 문서 1412
자세히 알아보기 1413
AWSBillingReadOnlyAccess 1413
이 정책 사용 1413
정책 세부 정보 1413
정책 버전 1413
JSON 정책 문서 1414
자세히 알아보기 1415
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1415
이 정책 사용 1415
정책 세부 정보 1415
정책 버전 1416
JSON 정책 문서 1416
자세히 알아보기 1417
AWSBudgetsActionsWithAWSResourceControlAccess 1417
이 정책 사용 1417
정책 세부 정보 1417
정책 버전 1418
JSON 정책 문서 1418
자세히 알아보기 1419
AWSBudgetsReadOnlyAccess 1419
이 정책 사용 1419
정책 세부 정보 1419
정책 버전 1420
JSON 정책 문서 1420
자세히 알아보기 1420
AWSBugBustFullAccess 1420
이 정책 사용 1421
정책 세부 정보 1421
정책 버전 1421
JSON 정책 문서 1421
자세히 알아보기 1422

AWSBugBustPlayerAccess 1422
이 정책 사용 1423
정책 세부 정보 1423
정책 버전 1423
JSON 정책 문서 1423
자세히 알아보기 1424
AWSBugBustServiceRolePolicy 1424
이 정책 사용 1424
정책 세부 정보 1425
정책 버전 1425
JSON 정책 문서 1425
자세히 알아보기 1425
AWSCertificateManagerFullAccess 1426
이 정책 사용 1426
정책 세부 정보 1426
정책 버전 1426
JSON 정책 문서 1426
자세히 알아보기 1427
AWSCertificateManagerPrivateCAAuditor 1427
이 정책 사용 1427
정책 세부 정보 1428
정책 버전 1428
JSON 정책 문서 1428
자세히 알아보기 1429
AWSCertificateManagerPrivateCAFullAccess 1429
이 정책 사용 1429
정책 세부 정보 1429
정책 버전 1429
JSON 정책 문서 1430
자세히 알아보기 1430
AWSCertificateManagerPrivateCAPrivilegedUser 1430
이 정책 사용 1430
정책 세부 정보 1430
정책 버전 1431
JSON 정책 문서 1431
자세히 알아보기 1432

AWSCertificateManagerPrivateCAReadOnly 1432
이 정책 사용 1432
정책 세부 정보 1432
정책 버전 1433
JSON 정책 문서 1433
자세히 알아보기 1433
AWSCertificateManagerPrivateCAUser 1434
이 정책 사용 1434
정책 세부 정보 1434
정책 버전 1434
JSON 정책 문서 1434
자세히 알아보기 1435
AWSCertificateManagerReadOnly 1436
이 정책 사용 1436
정책 세부 정보 1436
정책 버전 1436
JSON 정책 문서 1436
자세히 알아보기 1437
AWSChatbotServiceLinkedRolePolicy 1437
이 정책 사용 1437
정책 세부 정보 1437
정책 버전 1437
JSON 정책 문서 1438
자세히 알아보기 1438
AWSCleanRoomsFullAccess 1438
이 정책 사용 1439
정책 세부 정보 1439
정책 버전 1439
JSON 정책 문서 1439
자세히 알아보기 1443
AWSCleanRoomsFullAccessNoQuerying 1444
이 정책 사용 1444
정책 세부 정보 1444
정책 버전 1444
JSON 정책 문서 1444
자세히 알아보기 1449

AWSCleanRoomsMLFullAccess 1449
이 정책 사용 1449
정책 세부 정보 1449
정책 버전 1450
JSON 정책 문서 1450
자세히 알아보기 1453
AWSCleanRoomsMLReadOnlyAccess 1454
이 정책 사용 1454
정책 세부 정보 1454
정책 버전 1454
JSON 정책 문서 1454
자세히 알아보기 1455
AWSCleanRoomsReadOnlyAccess 1455
이 정책 사용 1455
정책 세부 정보 1456
정책 버전 1456
JSON 정책 문서 1456
자세히 알아보기 1457
AWSCloud9Administrator 1457
이 정책 사용 1457
정책 세부 정보 1458
정책 버전 1458
JSON 정책 문서 1458
자세히 알아보기 1459
AWSCloud9EnvironmentMember 1460
이 정책 사용 1460
정책 세부 정보 1460
정책 버전 1460
JSON 정책 문서 1460
자세히 알아보기 1462
AWSCloud9ServiceRolePolicy 1462
이 정책 사용 1462
정책 세부 정보 1462
정책 버전 1462
JSON 정책 문서 1462
자세히 알아보기 1465

AWSCloud9SSMInstanceProfile 1465
이 정책 사용 1465
정책 세부 정보 1465
정책 버전 1465
JSON 정책 문서 1466
자세히 알아보기 1466
AWSCloud9User 1466
이 정책 사용 1466
정책 세부 정보 1467
정책 버전 1467
JSON 정책 문서 1467
자세히 알아보기 1469
AWSCloudFormationFullAccess 1470
이 정책 사용 1470
정책 세부 정보 1470
정책 버전 1470
JSON 정책 문서 1470
자세히 알아보기 1471
AWSCloudFormationReadOnlyAccess 1471
이 정책 사용 1471
정책 세부 정보 1471
정책 버전 1471
JSON 정책 문서 1471
자세히 알아보기 1472
AWSCloudFrontLogger 1472
이 정책 사용 1472
정책 세부 정보 1472
정책 버전 1473
JSON 정책 문서 1473
자세히 알아보기 1473
AWSCloudHSMFullAccess 1473
이 정책 사용 1473
정책 세부 정보 1474
정책 버전 1474
JSON 정책 문서 1474
자세히 알아보기 1474

AWSCloudHSMReadOnlyAccess 1475
이 정책 사용 1475
정책 세부 정보 1475
정책 버전 1475
JSON 정책 문서 1475
자세히 알아보기 1476
AWSCloudHSMRole 1476
이 정책 사용 1476
정책 세부 정보 1476
정책 버전 1476
JSON 정책 문서 1476
자세히 알아보기 1477
AWSCloudMapDiscoverInstanceAccess 1477
이 정책 사용 1477
정책 세부 정보 1477
정책 버전 1478
JSON 정책 문서 1478
자세히 알아보기 1478
AWSCloudMapFullAccess 1479
이 정책 사용 1479
정책 세부 정보 1479
정책 버전 1479
JSON 정책 문서 1479
자세히 알아보기 1480
AWSCloudMapReadOnlyAccess 1480
이 정책 사용 1480
정책 세부 정보 1480
정책 버전 1481
JSON 정책 문서 1481
자세히 알아보기 1481
AWSCloudMapRegisterInstanceAccess 1481
이 정책 사용 1482
정책 세부 정보 1482
정책 버전 1482
JSON 정책 문서 1482
자세히 알아보기 1483

AWSCloudShellFullAccess 1483
이 정책 사용 1483
정책 세부 정보 1483
정책 버전 1483
JSON 정책 문서 1484
자세히 알아보기 1484
AWSCloudTrail_FullAccess 1484
이 정책 사용 1484
정책 세부 정보 1484
정책 버전 1485
JSON 정책 문서 1485
자세히 알아보기 1487
AWSCloudTrail_ReadOnlyAccess 1488
이 정책 사용 1488
정책 세부 정보 1488
정책 버전 1488
JSON 정책 문서 1488
자세히 알아보기 1489
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1489
이 정책 사용 1489
정책 세부 정보 1489
정책 버전 1489
JSON 정책 문서 1490
자세히 알아보기 1490
AWSCodeArtifactAdminAccess 1490
이 정책 사용 1490
정책 세부 정보 1490
정책 버전 1491
JSON 정책 문서 1491
자세히 알아보기 1491
AWSCodeArtifactReadOnlyAccess 1492
이 정책 사용 1492
정책 세부 정보 1492
정책 버전 1492
JSON 정책 문서 1492
자세히 알아보기 1493

AWSCodeBuildAdminAccess 1493
이 정책 사용 1493
정책 세부 정보 1493
정책 버전 1494
JSON 정책 문서 1494
자세히 알아보기 1497
AWSCodeBuildDeveloperAccess 1497
이 정책 사용 1497
정책 세부 정보 1498
정책 버전 1498
JSON 정책 문서 1498
자세히 알아보기 1500
AWSCodeBuildReadOnlyAccess 1501
이 정책 사용 1501
정책 세부 정보 1501
정책 버전 1501
JSON 정책 문서 1501
자세히 알아보기 1503
AWSCodeCommitFullAccess 1503
이 정책 사용 1503
정책 세부 정보 1503
정책 버전 1503
JSON 정책 문서 1504
자세히 알아보기 1508
AWSCodeCommitPowerUser 1508
이 정책 사용 1508
정책 세부 정보 1509
정책 버전 1509
JSON 정책 문서 1509
자세히 알아보기 1514
AWSCodeCommitReadOnly 1514
이 정책 사용 1514
정책 세부 정보 1514
정책 버전 1514
JSON 정책 문서 1515
자세히 알아보기 1517

AWSCodeDeployDeployerAccess 1517
이 정책 사용 1517
정책 세부 정보 1518
정책 버전 1518
JSON 정책 문서 1518
자세히 알아보기 1519
AWSCodeDeployFullAccess 1520
이 정책 사용 1520
정책 세부 정보 1520
정책 버전 1520
JSON 정책 문서 1520
자세히 알아보기 1522
AWSCodeDeployReadOnlyAccess 1522
이 정책 사용 1522
정책 세부 정보 1522
정책 버전 1522
JSON 정책 문서 1523
자세히 알아보기 1524
AWSCodeDeployRole 1524
이 정책 사용 1524
정책 세부 정보 1524
정책 버전 1524
JSON 정책 문서 1524
자세히 알아보기 1526
AWSCodeDeployRoleForCloudFormation 1526
이 정책 사용 1526
정책 세부 정보 1526
정책 버전 1526
JSON 정책 문서 1527
자세히 알아보기 1527
AWSCodeDeployRoleForECS 1527
이 정책 사용 1527
정책 세부 정보 1528
정책 버전 1528
JSON 정책 문서 1528
자세히 알아보기 1529

AWSCodeDeployRoleForECSLimited 1529
이 정책 사용 1529
정책 세부 정보 1529
정책 버전 1530
JSON 정책 문서 1530
자세히 알아보기 1531
AWSCodeDeployRoleForLambda 1532
이 정책 사용 1532
정책 세부 정보 1532
정책 버전 1532
JSON 정책 문서 1532
자세히 알아보기 1533
AWSCodeDeployRoleForLambdaLimited 1534
이 정책 사용 1534
정책 세부 정보 1534
정책 버전 1534
JSON 정책 문서 1534
자세히 알아보기 1535
AWSCodePipeline_FullAccess 1536
이 정책 사용 1536
정책 세부 정보 1536
정책 버전 1536
JSON 정책 문서 1536
자세히 알아보기 1540
AWSCodePipeline_ReadOnlyAccess 1540
이 정책 사용 1540
정책 세부 정보 1540
정책 버전 1541
JSON 정책 문서 1541
자세히 알아보기 1542
AWSCodePipelineApproverAccess 1542
이 정책 사용 1542
정책 세부 정보 1542
정책 버전 1543
JSON 정책 문서 1543
자세히 알아보기 1543

AWSCodePipelineCustomActionAccess 1544
이 정책 사용 1544
정책 세부 정보 1544
정책 버전 1544
JSON 정책 문서 1544
자세히 알아보기 1545
AWSCodeStarFullAccess 1545
이 정책 사용 1545
정책 세부 정보 1545
정책 버전 1545
JSON 정책 문서 1546
자세히 알아보기 1546
AWSCodeStarNotificationsServiceRolePolicy 1547
이 정책 사용 1547
정책 세부 정보 1547
정책 버전 1547
JSON 정책 문서 1547
자세히 알아보기 1548
AWSCodeStarServiceRole 1549
이 정책 사용 1549
정책 세부 정보 1549
정책 버전 1549
JSON 정책 문서 1549
자세히 알아보기 1554
AWSCompromisedKeyQuarantine 1554
이 정책 사용 1554
정책 세부 정보 1554
정책 버전 1555
JSON 정책 문서 1555
자세히 알아보기 1556
AWSCompromisedKeyQuarantineV2 1556
이 정책 사용 1556
정책 세부 정보 1556
정책 버전 1557
JSON 정책 문서 1557
자세히 알아보기 1559

AWSConfigMultiAccountSetupPolicy 1559
이 정책 사용 1559
정책 세부 정보 1559
정책 버전 1559
JSON 정책 문서 1559
자세히 알아보기 1561
AWSConfigRemediationServiceRolePolicy 1562
이 정책 사용 1562
정책 세부 정보 1562
정책 버전 1562
JSON 정책 문서 1562
자세히 알아보기 1563
AWSConfigRoleForOrganizations 1563
이 정책 사용 1563
정책 세부 정보 1563
정책 버전 1563
JSON 정책 문서 1564
자세히 알아보기 1564
AWSConfigRulesExecutionRole 1564
이 정책 사용 1564
정책 세부 정보 1565
정책 버전 1565
JSON 정책 문서 1565
자세히 알아보기 1566
AWSConfigServiceRolePolicy 1566
이 정책 사용 1566
정책 세부 정보 1566
정책 버전 1566
JSON 정책 문서 1566
자세히 알아보기 1598
AWSConfigUserAccess 1598
이 정책 사용 1598
정책 세부 정보 1598
정책 버전 1599
JSON 정책 문서 1599
자세히 알아보기 1599

AWSConnector 1600
이 정책 사용 1600
정책 세부 정보 1600
정책 버전 1600
JSON 정책 문서 1600
자세히 알아보기 1602
AWSControlTowerAccountServiceRolePolicy 1602
이 정책 사용 1602
정책 세부 정보 1603
정책 버전 1603
JSON 정책 문서 1603
자세히 알아보기 1605
AWSControlTowerServiceRolePolicy 1605
이 정책 사용 1605
정책 세부 정보 1605
정책 버전 1605
JSON 정책 문서 1605
자세히 알아보기 1610
AWSCostAndUsageReportAutomationPolicy 1610
이 정책 사용 1610
정책 세부 정보 1610
정책 버전 1611
JSON 정책 문서 1611
자세히 알아보기 1612
AWSDataExchangeFullAccess 1612
이 정책 사용 1612
정책 세부 정보 1612
정책 버전 1612
JSON 정책 문서 1613
자세히 알아보기 1616
AWSDataExchangeProviderFullAccess 1616
이 정책 사용 1616
정책 세부 정보 1616
정책 버전 1616
JSON 정책 문서 1617
자세히 알아보기 1620

AWSDataExchangeReadOnly 1620
이 정책 사용 1620
정책 세부 정보 1621
정책 버전 1621
JSON 정책 문서 1621
자세히 알아보기 1622
AWSDataExchangeSubscriberFullAccess 1622
이 정책 사용 1622
정책 세부 정보 1622
정책 버전 1622
JSON 정책 문서 1623
자세히 알아보기 1625
AWSDataLifecycleManagerServiceRole 1625
이 정책 사용 1625
정책 세부 정보 1625
정책 버전 1625
JSON 정책 문서 1626
자세히 알아보기 1627
AWSDataLifecycleManagerServiceRoleForAMIManagement 1627
이 정책 사용 1627
정책 세부 정보 1627
정책 버전 1627
JSON 정책 문서 1628
자세히 알아보기 1629
AWSDataLifecycleManagerSSMFullAccess 1629
이 정책 사용 1629
정책 세부 정보 1629
정책 버전 1630
JSON 정책 문서 1630
자세히 알아보기 1631
AWSDataPipeline_FullAccess 1631
이 정책 사용 1631
정책 세부 정보 1632
정책 버전 1632
JSON 정책 문서 1632
자세히 알아보기 1633

AWSDataPipeline_PowerUser 1633
이 정책 사용 1633
정책 세부 정보 1633
정책 버전 1634
JSON 정책 문서 1634
자세히 알아보기 1635
AWSDataSyncDiscoveryServiceRolePolicy 1635
이 정책 사용 1635
정책 세부 정보 1635
정책 버전 1635
JSON 정책 문서 1636
자세히 알아보기 1637
AWSDataSyncFullAccess 1637
이 정책 사용 1637
정책 세부 정보 1637
정책 버전 1637
JSON 정책 문서 1637
자세히 알아보기 1639
AWSDataSyncReadOnlyAccess 1639
이 정책 사용 1639
정책 세부 정보 1639
정책 버전 1639
JSON 정책 문서 1639
자세히 알아보기 1640
AWSDeepLensLambdaFunctionAccessPolicy 1640
이 정책 사용 1640
정책 세부 정보 1641
정책 버전 1641
JSON 정책 문서 1641
자세히 알아보기 1642
AWSDeepLensServiceRolePolicy 1643
이 정책 사용 1643
정책 세부 정보 1643
정책 버전 1643
JSON 정책 문서 1643
자세히 알아보기 1650

AWSDeepRacerAccountAdminAccess 1650
이 정책 사용 1651
정책 세부 정보 1651
정책 버전 1651
JSON 정책 문서 1651
자세히 알아보기 1652
AWSDeepRacerCloudFormationAccessPolicy 1652
이 정책 사용 1652
정책 세부 정보 1652
정책 버전 1652
JSON 정책 문서 1652
자세히 알아보기 1655
AWSDeepRacerDefaultMultiUserAccess 1656
이 정책 사용 1656
정책 세부 정보 1656
정책 버전 1656
JSON 정책 문서 1656
자세히 알아보기 1658
AWSDeepRacerFullAccess 1658
이 정책 사용 1658
정책 세부 정보 1658
정책 버전 1658
JSON 정책 문서 1658
자세히 알아보기 1659
AWSDeepRacerRoboMakerAccessPolicy 1660
이 정책 사용 1660
정책 세부 정보 1660
정책 버전 1660
JSON 정책 문서 1660
자세히 알아보기 1662
AWSDeepRacerServiceRolePolicy 1662
이 정책 사용 1662
정책 세부 정보 1663
정책 버전 1663
JSON 정책 문서 1663
자세히 알아보기 1666

AWSDenyAll 1666
이 정책 사용 1666
정책 세부 정보 1666
정책 버전 1667
JSON 정책 문서 1667
자세히 알아보기 1667
AWSDeviceFarmFullAccess 1667
이 정책 사용 1668
정책 세부 정보 1668
정책 버전 1668
JSON 정책 문서 1668
자세히 알아보기 1668
AWSDeviceFarmServiceRolePolicy 1669
이 정책 사용 1669
정책 세부 정보 1669
정책 버전 1669
JSON 정책 문서 1669
자세히 알아보기 1671
AWSDeviceFarmTestGridServiceRolePolicy 1672
이 정책 사용 1672
정책 세부 정보 1672
정책 버전 1672
JSON 정책 문서 1672
자세히 알아보기 1674
AWSDirectConnectFullAccess 1674
이 정책 사용 1675
정책 세부 정보 1675
정책 버전 1675
JSON 정책 문서 1675
자세히 알아보기 1675
AWSDirectConnectReadOnlyAccess 1676
이 정책 사용 1676
정책 세부 정보 1676
정책 버전 1676
JSON 정책 문서 1676
자세히 알아보기 1677

AWSDirectConnectServiceRolePolicy 1677
이 정책 사용 1677
정책 세부 정보 1677
정책 버전 1677
JSON 정책 문서 1678
자세히 알아보기 1678
AWSDirectoryServiceFullAccess 1678
이 정책 사용 1678
정책 세부 정보 1678
정책 버전 1679
JSON 정책 문서 1679
자세히 알아보기 1681
AWSDirectoryServiceReadOnlyAccess 1681
이 정책 사용 1681
정책 세부 정보 1681
정책 버전 1681
JSON 정책 문서 1681
자세히 알아보기 1682
AWSDiscoveryContinuousExportFirehosePolicy 1682
이 정책 사용 1683
정책 세부 정보 1683
정책 버전 1683
JSON 정책 문서 1683
자세히 알아보기 1684
AWSDMSFleetAdvisorServiceRolePolicy 1684
이 정책 사용 1684
정책 세부 정보 1684
정책 버전 1685
JSON 정책 문서 1685
자세히 알아보기 1685
AWSDMSServerlessServiceRolePolicy 1685
이 정책 사용 1686
정책 세부 정보 1686
정책 버전 1686
JSON 정책 문서 1686
자세히 알아보기 1688

AWSEC2CapacityReservationFleetRolePolicy 1688
이 정책 사용 1688
정책 세부 정보 1688
정책 버전 1688
JSON 정책 문서 1688
자세히 알아보기 1689
AWSEC2FleetServiceRolePolicy 1690
이 정책 사용 1690
정책 세부 정보 1690
정책 버전 1690
JSON 정책 문서 1690
자세히 알아보기 1692
AWSEC2SpotFleetServiceRolePolicy 1692
이 정책 사용 1693
정책 세부 정보 1693
정책 버전 1693
JSON 정책 문서 1693
자세히 알아보기 1695
AWSEC2SpotServiceRolePolicy 1695
이 정책 사용 1695
정책 세부 정보 1695
정책 버전 1696
JSON 정책 문서 1696
자세히 알아보기 1697
AWSECRPullThroughCache_ServiceRolePolicy 1697
이 정책 사용 1698
정책 세부 정보 1698
정책 버전 1698
JSON 정책 문서 1698
자세히 알아보기 1699
AWSElasticBeanstalkCustomPlatformforEC2Role 1699
이 정책 사용 1699
정책 세부 정보 1699
정책 버전 1700
JSON 정책 문서 1700
자세히 알아보기 1701

AWSElasticBeanstalkEnhancedHealth 1702
이 정책 사용 1702
정책 세부 정보 1702
정책 버전 1702
JSON 정책 문서 1702
자세히 알아보기 1703
AWSElasticBeanstalkMaintenance 1703
이 정책 사용 1704
정책 세부 정보 1704
정책 버전 1704
JSON 정책 문서 1704
자세히 알아보기 1705
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 1705
이 정책 사용 1705
정책 세부 정보 1705
정책 버전 1706
JSON 정책 문서 1706
자세히 알아보기 1712
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 1713
이 정책 사용 1713
정책 세부 정보 1713
정책 버전 1713
JSON 정책 문서 1713
자세히 알아보기 1718
AWSElasticBeanstalkMulticontainerDocker 1719
이 정책 사용 1719
정책 세부 정보 1719
정책 버전 1719
JSON 정책 문서 1719
자세히 알아보기 1720
AWSElasticBeanstalkReadOnly 1721
이 정책 사용 1721
정책 세부 정보 1721
정책 버전 1721
JSON 정책 문서 1721
자세히 알아보기 1723

AWSElasticBeanstalkRoleCore 1724
이 정책 사용 1724
정책 세부 정보 1724
정책 버전 1724
JSON 정책 문서 1724
자세히 알아보기 1729
AWSElasticBeanstalkRoleCWL 1729
이 정책 사용 1729
정책 세부 정보 1729
정책 버전 1730
JSON 정책 문서 1730
자세히 알아보기 1730
AWSElasticBeanstalkRoleECS 1731
이 정책 사용 1731
정책 세부 정보 1731
정책 버전 1731
JSON 정책 문서 1731
자세히 알아보기 1732
AWSElasticBeanstalkRoleRDS 1732
이 정책 사용 1732
정책 세부 정보 1732
정책 버전 1733
JSON 정책 문서 1733
자세히 알아보기 1733
AWSElasticBeanstalkRoleSNS 1734
이 정책 사용 1734
정책 세부 정보 1734
정책 버전 1734
JSON 정책 문서 1734
자세히 알아보기 1735
AWSElasticBeanstalkRoleWorkerTier 1735
이 정책 사용 1735
정책 세부 정보 1735
정책 버전 1736
JSON 정책 문서 1736
자세히 알아보기 1737

AWSElasticBeanstalkService 1737
이 정책 사용 1737
정책 세부 정보 1737
정책 버전 1737
JSON 정책 문서 1738
자세히 알아보기 1742
AWSElasticBeanstalkServiceRolePolicy 1742
이 정책 사용 1742
정책 세부 정보 1742
정책 버전 1743
JSON 정책 문서 1743
자세히 알아보기 1744
AWSElasticBeanstalkWebTier 1744
이 정책 사용 1744
정책 세부 정보 1745
정책 버전 1745
JSON 정책 문서 1745
자세히 알아보기 1746
AWSElasticBeanstalkWorkerTier 1747
이 정책 사용 1747
정책 세부 정보 1747
정책 버전 1747
JSON 정책 문서 1747
자세히 알아보기 1749
AWSElasticDisasterRecoveryAgentInstallationPolicy 1750
이 정책 사용 1750
정책 세부 정보 1750
정책 버전 1750
JSON 정책 문서 1750
자세히 알아보기 1752
AWSElasticDisasterRecoveryAgentPolicy 1752
이 정책 사용 1752
정책 세부 정보 1752
정책 버전 1752
JSON 정책 문서 1753
자세히 알아보기 1753

AWSElasticDisasterRecoveryConsoleFullAccess 1754
이 정책 사용 1754
정책 세부 정보 1754
정책 버전 1754
JSON 정책 문서 1754
자세히 알아보기 1764
AWSElasticDisasterRecoveryConsoleFullAccess_v2 1764
이 정책 사용 1764
정책 세부 정보 1765
정책 버전 1765
JSON 정책 문서 1765
자세히 알아보기 1778
AWSElasticDisasterRecoveryConversionServerPolicy 1778
이 정책 사용 1778
정책 세부 정보 1778
정책 버전 1778
JSON 정책 문서 1779
자세히 알아보기 1779
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 1780
이 정책 사용 1780
정책 세부 정보 1780
정책 버전 1780
JSON 정책 문서 1780
자세히 알아보기 1781
AWSElasticDisasterRecoveryEc2InstancePolicy 1781
이 정책 사용 1781
정책 세부 정보 1782
정책 버전 1782
JSON 정책 문서 1782
자세히 알아보기 1784
AWSElasticDisasterRecoveryFailbackInstallationPolicy 1784
이 정책 사용 1784
정책 세부 정보 1784
정책 버전 1785
JSON 정책 문서 1785
자세히 알아보기 1786

AWSElasticDisasterRecoveryFailbackPolicy 1786
이 정책 사용 1786
정책 세부 정보 1786
정책 버전 1786
JSON 정책 문서 1787
자세히 알아보기 1788
AWSElasticDisasterRecoveryLaunchActionsPolicy 1788
이 정책 사용 1788
정책 세부 정보 1788
정책 버전 1789
JSON 정책 문서 1789
자세히 알아보기 1795
AWSElasticDisasterRecoveryNetworkReplicationPolicy 1795
이 정책 사용 1795
정책 세부 정보 1795
정책 버전 1795
JSON 정책 문서 1796
자세히 알아보기 1796
AWSElasticDisasterRecoveryReadOnlyAccess 1796
이 정책 사용 1797
정책 세부 정보 1797
정책 버전 1797
JSON 정책 문서 1797
자세히 알아보기 1799
AWSElasticDisasterRecoveryRecoveryInstancePolicy 1799
이 정책 사용 1800
정책 세부 정보 1800
정책 버전 1800
JSON 정책 문서 1800
자세히 알아보기 1803
AWSElasticDisasterRecoveryReplicationServerPolicy 1803
이 정책 사용 1803
정책 세부 정보 1803
정책 버전 1804
JSON 정책 문서 1804
자세히 알아보기 1806

AWSElasticDisasterRecoveryServiceRolePolicy 1806
이 정책 사용 1806
정책 세부 정보 1806
정책 버전 1807
JSON 정책 문서 1807
자세히 알아보기 1815
AWSElasticDisasterRecoveryStagingAccountPolicy 1815
이 정책 사용 1816
정책 세부 정보 1816
정책 버전 1816
JSON 정책 문서 1816
자세히 알아보기 1817
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 1817
이 정책 사용 1817
정책 세부 정보 1817
정책 버전 1818
JSON 정책 문서 1818
자세히 알아보기 1819
AWSElasticLoadBalancingClassicServiceRolePolicy 1819
이 정책 사용 1819
정책 세부 정보 1819
정책 버전 1820
JSON 정책 문서 1820
자세히 알아보기 1821
AWSElasticLoadBalancingServiceRolePolicy 1821
이 정책 사용 1821
정책 세부 정보 1821
정책 버전 1821
JSON 정책 문서 1822
자세히 알아보기 1823
AWSElementalMediaConvertFullAccess 1823
이 정책 사용 1823
정책 세부 정보 1823
정책 버전 1823
JSON 정책 문서 1823
자세히 알아보기 1824

AWSElementalMediaConvertReadOnly 1824
이 정책 사용 1825
정책 세부 정보 1825
정책 버전 1825
JSON 정책 문서 1825
자세히 알아보기 1826
AWSElementalMediaLiveFullAccess 1826
이 정책 사용 1826
정책 세부 정보 1826
정책 버전 1826
JSON 정책 문서 1826
자세히 알아보기 1827
AWSElementalMediaLiveReadOnly 1827
이 정책 사용 1827
정책 세부 정보 1827
정책 버전 1827
JSON 정책 문서 1828
자세히 알아보기 1828
AWSElementalMediaPackageFullAccess 1828
이 정책 사용 1828
정책 세부 정보 1828
정책 버전 1829
JSON 정책 문서 1829
자세히 알아보기 1829
AWSElementalMediaPackageReadOnly 1829
이 정책 사용 1829
정책 세부 정보 1829
정책 버전 1830
JSON 정책 문서 1830
자세히 알아보기 1830
AWSElementalMediaPackageV2FullAccess 1830
이 정책 사용 1831
정책 세부 정보 1831
정책 버전 1831
JSON 정책 문서 1831
자세히 알아보기 1831

AWSElementalMediaPackageV2ReadOnly 1832
이 정책 사용 1832
정책 세부 정보 1832
정책 버전 1832
JSON 정책 문서 1832
자세히 알아보기 1833
AWSElementalMediaStoreFullAccess 1833
이 정책 사용 1833
정책 세부 정보 1833
정책 버전 1833
JSON 정책 문서 1833
자세히 알아보기 1834
AWSElementalMediaStoreReadOnly 1834
이 정책 사용 1834
정책 세부 정보 1834
정책 버전 1835
JSON 정책 문서 1835
자세히 알아보기 1835
AWSElementalMediaTailorFullAccess 1836
이 정책 사용 1836
정책 세부 정보 1836
정책 버전 1836
JSON 정책 문서 1836
자세히 알아보기 1836
AWSElementalMediaTailorReadOnly 1837
이 정책 사용 1837
정책 세부 정보 1837
정책 버전 1837
JSON 정책 문서 1837
자세히 알아보기 1838
AWSEnhancedClassicNetworkingMangementPolicy 1838
이 정책 사용 1838
정책 세부 정보 1838
정책 버전 1838
JSON 정책 문서 1839
자세히 알아보기 1839

AWSEntityResolutionConsoleFullAccess 1839
이 정책 사용 1839
정책 세부 정보 1839
정책 버전 1840
JSON 정책 문서 1840
자세히 알아보기 1842
AWSEntityResolutionConsoleReadOnlyAccess 1843
이 정책 사용 1843
정책 세부 정보 1843
정책 버전 1843
JSON 정책 문서 1843
자세히 알아보기 1844
AWSFaultInjectionSimulatorEC2Access 1844
이 정책 사용 1844
정책 세부 정보 1844
정책 버전 1844
JSON 정책 문서 1845
자세히 알아보기 1846
AWSFaultInjectionSimulatorECSAccess 1846
이 정책 사용 1846
정책 세부 정보 1846
정책 버전 1847
JSON 정책 문서 1847
자세히 알아보기 1849
AWSFaultInjectionSimulatorEKSAccess 1849
이 정책 사용 1849
정책 세부 정보 1849
정책 버전 1849
JSON 정책 문서 1849
자세히 알아보기 1851
AWSFaultInjectionSimulatorNetworkAccess 1851
이 정책 사용 1851
정책 세부 정보 1851
정책 버전 1851
JSON 정책 문서 1851
자세히 알아보기 1858

AWSFaultInjectionSimulatorRDSAccess 1859
이 정책 사용 1859
정책 세부 정보 1859
정책 버전 1859
JSON 정책 문서 1859
자세히 알아보기 1860
AWSFaultInjectionSimulatorSSMAccess 1861
이 정책 사용 1861
정책 세부 정보 1861
정책 버전 1861
JSON 정책 문서 1861
자세히 알아보기 1862
AWSFinSpaceServiceRolePolicy 1863
이 정책 사용 1863
정책 세부 정보 1863
정책 버전 1863
JSON 정책 문서 1863
자세히 알아보기 1864
AWSFMAdminFullAccess 1864
이 정책 사용 1864
정책 세부 정보 1864
정책 버전 1864
JSON 정책 문서 1865
자세히 알아보기 1866
AWSFMAdminReadOnlyAccess 1867
이 정책 사용 1867
정책 세부 정보 1867
정책 버전 1867
JSON 정책 문서 1867
자세히 알아보기 1869
AWSFMMemberReadOnlyAccess 1869
이 정책 사용 1869
정책 세부 정보 1869
정책 버전 1869
JSON 정책 문서 1870
자세히 알아보기 1870

AWSForWordPressPluginPolicy 1870
이 정책 사용 1870
정책 세부 정보 1870
정책 버전 1871
JSON 정책 문서 1871
자세히 알아보기 1873
AWSGitSyncServiceRolePolicy 1873
이 정책 사용 1873
정책 세부 정보 1873
정책 버전 1873
JSON 정책 문서 1874
자세히 알아보기 1874
AWSGlobalAcceleratorSLRPolicy 1874
이 정책 사용 1874
정책 세부 정보 1874
정책 버전 1875
JSON 정책 문서 1875
자세히 알아보기 1876
AWSGlueConsoleFullAccess 1877
이 정책 사용 1877
정책 세부 정보 1877
정책 버전 1877
JSON 정책 문서 1877
자세히 알아보기 1881
AWSGlueConsoleSageMakerNotebookFullAccess 1882
이 정책 사용 1882
정책 세부 정보 1882
정책 버전 1882
JSON 정책 문서 1882
자세히 알아보기 1887
AwsGlueDataBrewFullAccessPolicy 1888
이 정책 사용 1888
정책 세부 정보 1888
정책 버전 1888
JSON 정책 문서 1888
자세히 알아보기 1893

AWSGlueDataBrewServiceRole 1894
이 정책 사용 1894
정책 세부 정보 1894
정책 버전 1894
JSON 정책 문서 1894
자세히 알아보기 1897
AWSGlueSchemaRegistryFullAccess 1897
이 정책 사용 1897
정책 세부 정보 1897
정책 버전 1898
JSON 정책 문서 1898
자세히 알아보기 1899
AWSGlueSchemaRegistryReadonlyAccess 1899
이 정책 사용 1899
정책 세부 정보 1899
정책 버전 1900
JSON 정책 문서 1900
자세히 알아보기 1901
AWSGlueServiceNotebookRole 1901
이 정책 사용 1901
정책 세부 정보 1901
정책 버전 1901
JSON 정책 문서 1901
자세히 알아보기 1904
AWSGlueServiceRole 1904
이 정책 사용 1904
정책 세부 정보 1904
정책 버전 1904
JSON 정책 문서 1905
자세히 알아보기 1907
AwsGlueSessionUserRestrictedNotebookPolicy 1907
이 정책 사용 1907
정책 세부 정보 1907
정책 버전 1907
JSON 정책 문서 1908
자세히 알아보기 1910

AwsGlueSessionUserRestrictedNotebookServiceRole 1910
이 정책 사용 1911
정책 세부 정보 1911
정책 버전 1911
JSON 정책 문서 1911
자세히 알아보기 1915
AwsGlueSessionUserRestrictedPolicy 1915
이 정책 사용 1915
정책 세부 정보 1915
정책 버전 1915
JSON 정책 문서 1916
자세히 알아보기 1918
AwsGlueSessionUserRestrictedServiceRole 1918
이 정책 사용 1918
정책 세부 정보 1918
정책 버전 1918
JSON 정책 문서 1919
자세히 알아보기 1922
AWSGrafanaAccountAdministrator 1922
이 정책 사용 1922
정책 세부 정보 1923
정책 버전 1923
JSON 정책 문서 1923
자세히 알아보기 1924
AWSGrafanaConsoleReadOnlyAccess 1924
이 정책 사용 1924
정책 세부 정보 1924
정책 버전 1925
JSON 정책 문서 1925
자세히 알아보기 1925
AWSGrafanaWorkspacePermissionManagement 1925
이 정책 사용 1926
정책 세부 정보 1926
정책 버전 1926
JSON 정책 문서 1926
자세히 알아보기 1927

AWSGrafanaWorkspacePermissionManagementV2 1927
이 정책 사용 1927
정책 세부 정보 1927
정책 버전 1928
JSON 정책 문서 1928
자세히 알아보기 1929
AWSGreengrassFullAccess 1929
이 정책 사용 1929
정책 세부 정보 1929
정책 버전 1929
JSON 정책 문서 1930
자세히 알아보기 1930
AWSGreengrassReadOnlyAccess 1930
이 정책 사용 1930
정책 세부 정보 1930
정책 버전 1931
JSON 정책 문서 1931
자세히 알아보기 1931
AWSGreengrassResourceAccessRolePolicy 1931
이 정책 사용 1932
정책 세부 정보 1932
정책 버전 1932
JSON 정책 문서 1932
자세히 알아보기 1934
AWSGroundStationAgentInstancePolicy 1935
이 정책 사용 1935
정책 세부 정보 1935
정책 버전 1935
JSON 정책 문서 1935
자세히 알아보기 1936
AWSHealth_EventProcessorServiceRolePolicy 1936
이 정책 사용 1936
정책 세부 정보 1936
정책 버전 1936
JSON 정책 문서 1937
자세히 알아보기 1937

AWSHealthFullAccess 1937
이 정책 사용 1938
정책 세부 정보 1938
정책 버전 1938
JSON 정책 문서 1938
자세히 알아보기 1939
AWSHealthImagingFullAccess 1939
이 정책 사용 1939
정책 세부 정보 1939
정책 버전 1940
JSON 정책 문서 1940
자세히 알아보기 1940
AWSHealthImagingReadOnlyAccess 1941
이 정책 사용 1941
정책 세부 정보 1941
정책 버전 1941
JSON 정책 문서 1941
자세히 알아보기 1942
AWSIAMIdentityCenterAllowListForIdentityContext 1942
이 정책 사용 1942
정책 세부 정보 1942
정책 버전 1943
JSON 정책 문서 1943
자세히 알아보기 1945
AWSIdentitySyncFullAccess 1945
이 정책 사용 1945
정책 세부 정보 1945
정책 버전 1945
JSON 정책 문서 1945
자세히 알아보기 1946
AWSIdentitySyncReadOnlyAccess 1946
이 정책 사용 1947
정책 세부 정보 1947
정책 버전 1947
JSON 정책 문서 1947
자세히 알아보기 1947

AWSImageBuilderFullAccess 1948
이 정책 사용 1948
정책 세부 정보 1948
정책 버전 1948
JSON 정책 문서 1948
자세히 알아보기 1951
AWSImageBuilderReadOnlyAccess 1951
이 정책 사용 1951
정책 세부 정보 1951
정책 버전 1952
JSON 정책 문서 1952
자세히 알아보기 1952
AWSImportExportFullAccess 1953
이 정책 사용 1953
정책 세부 정보 1953
정책 버전 1953
JSON 정책 문서 1953
자세히 알아보기 1954
AWSImportExportReadOnlyAccess 1954
이 정책 사용 1954
정책 세부 정보 1954
정책 버전 1954
JSON 정책 문서 1954
자세히 알아보기 1955
AWSIncidentManagerIncidentAccessServiceRolePolicy 1955
이 정책 사용 1955
정책 세부 정보 1955
정책 버전 1956
JSON 정책 문서 1956
자세히 알아보기 1956
AWSIncidentManagerResolverAccess 1957
이 정책 사용 1957
정책 세부 정보 1957
정책 버전 1957
JSON 정책 문서 1957
자세히 알아보기 1958

AWSIncidentManagerServiceRolePolicy 1958
이 정책 사용 1959
정책 세부 정보 1959
정책 버전 1959
JSON 정책 문서 1959
자세히 알아보기 1960
AWSIoT1ClickFullAccess 1960
이 정책 사용 1960
정책 세부 정보 1961
정책 버전 1961
JSON 정책 문서 1961
자세히 알아보기 1961
AWSIoT1ClickReadOnlyAccess 1962
이 정책 사용 1962
정책 세부 정보 1962
정책 버전 1962
JSON 정책 문서 1962
자세히 알아보기 1963
AWSIoTAnalyticsFullAccess 1963
이 정책 사용 1963
정책 세부 정보 1963
정책 버전 1963
JSON 정책 문서 1963
자세히 알아보기 1964
AWSIoTAnalyticsReadOnlyAccess 1964
이 정책 사용 1964
정책 세부 정보 1964
정책 버전 1964
JSON 정책 문서 1965
자세히 알아보기 1965
AWSIoTConfigAccess 1965
이 정책 사용 1965
정책 세부 정보 1966
정책 버전 1966
JSON 정책 문서 1966
자세히 알아보기 1970

AWSIoTConfigReadOnlyAccess 1970
이 정책 사용 1970
정책 세부 정보 1970
정책 버전 1970
JSON 정책 문서 1971
자세히 알아보기 1973
AWSIoTDataAccess 1973
이 정책 사용 1973
정책 세부 정보 1973
정책 버전 1973
JSON 정책 문서 1973
자세히 알아보기 1974
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 1974
이 정책 사용 1974
정책 세부 정보 1974
정책 버전 1975
JSON 정책 문서 1975
자세히 알아보기 1975
AWSIoTDeviceDefenderAudit 1976
이 정책 사용 1976
정책 세부 정보 1976
정책 버전 1976
JSON 정책 문서 1976
자세히 알아보기 1977
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 1977
이 정책 사용 1977
정책 세부 정보 1977
정책 버전 1978
JSON 정책 문서 1978
자세히 알아보기 1979
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 1979
이 정책 사용 1979
정책 세부 정보 1979
정책 버전 1979
JSON 정책 문서 1980
자세히 알아보기 1980

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 1980
이 정책 사용 1980
정책 세부 정보 1981
정책 버전 1981
JSON 정책 문서 1981
자세히 알아보기 1981
AWSIoTDeviceDefenderUpdateCACertMitigationAction 1982
이 정책 사용 1982
정책 세부 정보 1982
정책 버전 1982
JSON 정책 문서 1982
자세히 알아보기 1983
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 1983
이 정책 사용 1983
정책 세부 정보 1983
정책 버전 1983
JSON 정책 문서 1984
자세히 알아보기 1984
AWSIoTDeviceTesterForFreeRTOSFullAccess 1984
이 정책 사용 1984
정책 세부 정보 1985
정책 버전 1985
JSON 정책 문서 1985
자세히 알아보기 1991
AWSIoTDeviceTesterForGreengrassFullAccess 1991
이 정책 사용 1991
정책 세부 정보 1992
정책 버전 1992
JSON 정책 문서 1992
자세히 알아보기 1995
AWSIoTEventsFullAccess 1995
이 정책 사용 1995
정책 세부 정보 1995
정책 버전 1995
JSON 정책 문서 1996
자세히 알아보기 1996

AWSIoTEventsReadOnlyAccess 1996
이 정책 사용 1996
정책 세부 정보 1996
정책 버전 1997
JSON 정책 문서 1997
자세히 알아보기 1997
AWSIoTFleetHubFederationAccess 1997
이 정책 사용 1998
정책 세부 정보 1998
정책 버전 1998
JSON 정책 문서 1998
자세히 알아보기 2000
AWSIoTFleetwiseServiceRolePolicy 2000
이 정책 사용 2000
정책 세부 정보 2000
정책 버전 2000
JSON 정책 문서 2001
자세히 알아보기 2001
AWSIoTFullAccess 2001
이 정책 사용 2001
정책 세부 정보 2002
정책 버전 2002
JSON 정책 문서 2002
자세히 알아보기 2002
AWSIoTLogging 2003
이 정책 사용 2003
정책 세부 정보 2003
정책 버전 2003
JSON 정책 문서 2003
자세히 알아보기 2004
AWSIoTOTAUpdate 2004
이 정책 사용 2004
정책 세부 정보 2004
정책 버전 2004
JSON 정책 문서 2005
자세히 알아보기 2005

AWSIotRoboRunnerFullAccess 2005
이 정책 사용 2005
정책 세부 정보 2005
정책 버전 2006
JSON 정책 문서 2006
자세히 알아보기 2006
AWSIotRoboRunnerReadOnly 2007
이 정책 사용 2007
정책 세부 정보 2007
정책 버전 2007
JSON 정책 문서 2007
자세히 알아보기 2008
AWSIotRoboRunnerServiceRolePolicy 2008
이 정책 사용 2008
정책 세부 정보 2008
정책 버전 2008
JSON 정책 문서 2009
자세히 알아보기 2009
AWSIoTRuleActions 2009
이 정책 사용 2009
정책 세부 정보 2010
정책 버전 2010
JSON 정책 문서 2010
자세히 알아보기 2010
AWSIoTSiteWiseConsoleFullAccess 2011
이 정책 사용 2011
정책 세부 정보 2011
정책 버전 2011
JSON 정책 문서 2011
자세히 알아보기 2013
AWSIoTSiteWiseFullAccess 2014
이 정책 사용 2014
정책 세부 정보 2014
정책 버전 2014
JSON 정책 문서 2014
자세히 알아보기 2015

AWSIoTSiteWiseMonitorPortalAccess 2015
이 정책 사용 2015
정책 세부 정보 2015
정책 버전 2015
JSON 정책 문서 2016
자세히 알아보기 2017
AWSIoTSiteWiseMonitorServiceRolePolicy 2017
이 정책 사용 2017
정책 세부 정보 2017
정책 버전 2017
JSON 정책 문서 2017
자세히 알아보기 2018
AWSIoTSiteWiseReadOnlyAccess 2019
이 정책 사용 2019
정책 세부 정보 2019
정책 버전 2019
JSON 정책 문서 2019
자세히 알아보기 2020
AWSIoTThingsRegistration 2020
이 정책 사용 2020
정책 세부 정보 2020
정책 버전 2020
JSON 정책 문서 2020
자세히 알아보기 2022
AWSIoTTwinMakerServiceRolePolicy 2022
이 정책 사용 2022
정책 세부 정보 2022
정책 버전 2022
JSON 정책 문서 2022
자세히 알아보기 2024
AWSIoTWirelessDataAccess 2024
이 정책 사용 2024
정책 세부 정보 2024
정책 버전 2025
JSON 정책 문서 2025
자세히 알아보기 2025

AWSIoTWirelessFullAccess 2025
이 정책 사용 2025
정책 세부 정보 2026
정책 버전 2026
JSON 정책 문서 2026
자세히 알아보기 2026
AWSIoTWirelessFullPublishAccess 2027
이 정책 사용 2027
정책 세부 정보 2027
정책 버전 2027
JSON 정책 문서 2027
자세히 알아보기 2028
AWSIoTWirelessGatewayCertManager 2028
이 정책 사용 2028
정책 세부 정보 2028
정책 버전 2028
JSON 정책 문서 2028
자세히 알아보기 2029
AWSIoTWirelessLogging 2029
이 정책 사용 2029
정책 세부 정보 2029
정책 버전 2029
JSON 정책 문서 2030
자세히 알아보기 2030
AWSIoTWirelessReadOnlyAccess 2030
이 정책 사용 2030
정책 세부 정보 2031
정책 버전 2031
JSON 정책 문서 2031
자세히 알아보기 2031
AWSIPAMServiceRolePolicy 2032
이 정책 사용 2032
정책 세부 정보 2032
정책 버전 2032
JSON 정책 문서 2032
자세히 알아보기 2033

AWSIQContractServiceRolePolicy 2033
이 정책 사용 2034
정책 세부 정보 2034
정책 버전 2034
JSON 정책 문서 2034
자세히 알아보기 2034
AWSIQFullAccess 2035
이 정책 사용 2035
정책 세부 정보 2035
정책 버전 2035
JSON 정책 문서 2035
자세히 알아보기 2036
AWSIQPermissionServiceRolePolicy 2036
이 정책 사용 2036
정책 세부 정보 2036
정책 버전 2037
JSON 정책 문서 2037
자세히 알아보기 2038
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2038
이 정책 사용 2038
정책 세부 정보 2038
정책 버전 2038
JSON 정책 문서 2038
자세히 알아보기 2039
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2039
이 정책 사용 2039
정책 세부 정보 2039
정책 버전 2040
JSON 정책 문서 2040
자세히 알아보기 2040
AWSKeyManagementServicePowerUser 2040
이 정책 사용 2041
정책 세부 정보 2041
정책 버전 2041
JSON 정책 문서 2041
자세히 알아보기 2042

AWSLakeFormationCrossAccountManager 2042
이 정책 사용 2042
정책 세부 정보 2042
정책 버전 2042
JSON 정책 문서 2043
자세히 알아보기 2044
AWSLakeFormationDataAdmin 2045
이 정책 사용 2045
정책 세부 정보 2045
정책 버전 2045
JSON 정책 문서 2045
자세히 알아보기 2046
AWSLambda_FullAccess 2047
이 정책 사용 2047
정책 세부 정보 2047
정책 버전 2047
JSON 정책 문서 2047
자세히 알아보기 2049
AWSLambda_ReadOnlyAccess 2049
이 정책 사용 2049
정책 세부 정보 2049
정책 버전 2049
JSON 정책 문서 2049
자세히 알아보기 2051
AWSLambdaBasicExecutionRole 2051
이 정책 사용 2051
정책 세부 정보 2051
정책 버전 2051
JSON 정책 문서 2051
자세히 알아보기 2052
AWSLambdaDynamoDBExecutionRole 2052
이 정책 사용 2052
정책 세부 정보 2052
정책 버전 2053
JSON 정책 문서 2053
자세히 알아보기 2053

AWSLambdaENIManagementAccess 2054
이 정책 사용 2054
정책 세부 정보 2054
정책 버전 2054
JSON 정책 문서 2054
자세히 알아보기 2055
AWSLambdaExecute 2055
이 정책 사용 2055
정책 세부 정보 2055
정책 버전 2055
JSON 정책 문서 2056
자세히 알아보기 2056
AWSLambdaFullAccess 2056
이 정책 사용 2056
정책 세부 정보 2057
정책 버전 2057
JSON 정책 문서 2057
자세히 알아보기 2059
AWSLambdaInvocation-DynamoDB 2059
이 정책 사용 2059
정책 세부 정보 2059
정책 버전 2059
JSON 정책 문서 2059
자세히 알아보기 2060
AWSLambdaKinesisExecutionRole 2060
이 정책 사용 2060
정책 세부 정보 2060
정책 버전 2061
JSON 정책 문서 2061
자세히 알아보기 2061
AWSLambdaMSKExecutionRole 2062
이 정책 사용 2062
정책 세부 정보 2062
정책 버전 2062
JSON 정책 문서 2062
자세히 알아보기 2063

AWSLambdaReplicator 2063
이 정책 사용 2063
정책 세부 정보 2063
정책 버전 2064
JSON 정책 문서 2064
자세히 알아보기 2065
AWSLambdaRole 2065
이 정책 사용 2065
정책 세부 정보 2065
정책 버전 2065
JSON 정책 문서 2066
자세히 알아보기 2066
AWSLambdaSQSQueueExecutionRole 2066
이 정책 사용 2066
정책 세부 정보 2066
정책 버전 2067
JSON 정책 문서 2067
자세히 알아보기 2067
AWSLambdaVPCAccessExecutionRole 2068
이 정책 사용 2068
정책 세부 정보 2068
정책 버전 2068
JSON 정책 문서 2068
자세히 알아보기 2069
AWSLicenseManagerConsumptionPolicy 2069
이 정책 사용 2069
정책 세부 정보 2069
정책 버전 2069
JSON 정책 문서 2070
자세히 알아보기 2070
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2070
이 정책 사용 2070
정책 세부 정보 2071
정책 버전 2071
JSON 정책 문서 2071
자세히 알아보기 2072

AWSLicenseManagerMasterAccountRolePolicy 2072
이 정책 사용 2072
정책 세부 정보 2072
정책 버전 2073
JSON 정책 문서 2073
자세히 알아보기 2078
AWSLicenseManagerMemberAccountRolePolicy 2078
이 정책 사용 2078
정책 세부 정보 2078
정책 버전 2078
JSON 정책 문서 2078
자세히 알아보기 2079
AWSLicenseManagerServiceRolePolicy 2080
이 정책 사용 2080
정책 세부 정보 2080
정책 버전 2080
JSON 정책 문서 2080
자세히 알아보기 2083
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2084
이 정책 사용 2084
정책 세부 정보 2084
정책 버전 2084
JSON 정책 문서 2084
자세히 알아보기 2086
AWSM2ServicePolicy 2086
이 정책 사용 2086
정책 세부 정보 2087
정책 버전 2087
JSON 정책 문서 2087
자세히 알아보기 2088
AWSManagedServices_ContactsServiceRolePolicy 2088
이 정책 사용 2089
정책 세부 정보 2089
정책 버전 2089
JSON 정책 문서 2089
자세히 알아보기 2090

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2090
이 정책 사용 2090
정책 세부 정보 2090
정책 버전 2091
JSON 정책 문서 2091
자세히 알아보기 2092
AWSManagedServices_EventsServiceRolePolicy 2092
이 정책 사용 2093
정책 세부 정보 2093
정책 버전 2093
JSON 정책 문서 2093
자세히 알아보기 2094
AWSManagedServicesDeploymentToolkitPolicy 2094
이 정책 사용 2094
정책 세부 정보 2094
정책 버전 2094
JSON 정책 문서 2095
자세히 알아보기 2097
AWSMarketplaceAmiIngestion 2097
이 정책 사용 2097
정책 세부 정보 2097
정책 버전 2097
JSON 정책 문서 2097
자세히 알아보기 2098
AWSMarketplaceDeploymentServiceRolePolicy 2098
이 정책 사용 2098
정책 세부 정보 2098
정책 버전 2099
JSON 정책 문서 2099
자세히 알아보기 2100
AWSMarketplaceFullAccess 2100
이 정책 사용 2101
정책 세부 정보 2101
정책 버전 2101
JSON 정책 문서 2101
자세히 알아보기 2104

AWSMarketplaceGetEntitlements 2104
이 정책 사용 2105
정책 세부 정보 2105
정책 버전 2105
JSON 정책 문서 2105
자세히 알아보기 2105
AWSMarketplaceImageBuildFullAccess 2106
이 정책 사용 2106
정책 세부 정보 2106
정책 버전 2106
JSON 정책 문서 2106
자세히 알아보기 2110
AWSMarketplaceLicenseManagementServiceRolePolicy 2110
이 정책 사용 2110
정책 세부 정보 2110
정책 버전 2110
JSON 정책 문서 2111
자세히 알아보기 2111
AWSMarketplaceManageSubscriptions 2111
이 정책 사용 2112
정책 세부 정보 2112
정책 버전 2112
JSON 정책 문서 2112
자세히 알아보기 2113
AWSMarketplaceMeteringFullAccess 2113
이 정책 사용 2113
정책 세부 정보 2113
정책 버전 2113
JSON 정책 문서 2114
자세히 알아보기 2114
AWSMarketplaceMeteringRegisterUsage 2114
이 정책 사용 2114
정책 세부 정보 2114
정책 버전 2115
JSON 정책 문서 2115
자세히 알아보기 2115

AWSMarketplaceProcurementSystemAdminFullAccess 2115
이 정책 사용 2116
정책 세부 정보 2116
정책 버전 2116
JSON 정책 문서 2116
자세히 알아보기 2117
AWSMarketplacePurchaseOrdersServiceRolePolicy 2117
이 정책 사용 2117
정책 세부 정보 2117
정책 버전 2117
JSON 정책 문서 2118
자세히 알아보기 2118
AWSMarketplaceRead-only 2118
이 정책 사용 2118
정책 세부 정보 2118
정책 버전 2119
JSON 정책 문서 2119
자세히 알아보기 2120
AWSMarketplaceResaleAuthorizationServiceRolePolicy 2120
이 정책 사용 2120
정책 세부 정보 2120
정책 버전 2121
JSON 정책 문서 2121
자세히 알아보기 2123
AWSMarketplaceSellerFullAccess 2123
이 정책 사용 2123
정책 세부 정보 2123
정책 버전 2124
JSON 정책 문서 2124
자세히 알아보기 2127
AWSMarketplaceSellerProductsFullAccess 2128
이 정책 사용 2128
정책 세부 정보 2128
정책 버전 2128
JSON 정책 문서 2128
자세히 알아보기 2130

AWSMarketplaceSellerProductsReadOnly 2130
이 정책 사용 2130
정책 세부 정보 2130
정책 버전 2131
JSON 정책 문서 2131
자세히 알아보기 2132
AWSMediaConnectServicePolicy 2132
이 정책 사용 2132
정책 세부 정보 2132
정책 버전 2132
JSON 정책 문서 2132
자세히 알아보기 2134
AWSMediaTailorServiceRolePolicy 2134
이 정책 사용 2134
정책 세부 정보 2134
정책 버전 2134
JSON 정책 문서 2134
자세히 알아보기 2135
AWSMigrationHubDiscoveryAccess 2135
이 정책 사용 2135
정책 세부 정보 2135
정책 버전 2136
JSON 정책 문서 2136
자세히 알아보기 2137
AWSMigrationHubDMSAccess 2137
이 정책 사용 2137
정책 세부 정보 2137
정책 버전 2138
JSON 정책 문서 2138
자세히 알아보기 2139
AWSMigrationHubFullAccess 2139
이 정책 사용 2139
정책 세부 정보 2139
정책 버전 2139
JSON 정책 문서 2140
자세히 알아보기 2141

AWSMigrationHubOrchestratorConsoleFullAccess 2141
이 정책 사용 2141
정책 세부 정보 2142
정책 버전 2142
JSON 정책 문서 2142
자세히 알아보기 2145
AWSMigrationHubOrchestratorInstanceRolePolicy 2145
이 정책 사용 2145
정책 세부 정보 2145
정책 버전 2146
JSON 정책 문서 2146
자세히 알아보기 2147
AWSMigrationHubOrchestratorPlugin 2147
이 정책 사용 2147
정책 세부 정보 2147
정책 버전 2147
JSON 정책 문서 2147
자세히 알아보기 2149
AWSMigrationHubOrchestratorServiceRolePolicy 2149
이 정책 사용 2149
정책 세부 정보 2149
정책 버전 2149
JSON 정책 문서 2150
자세히 알아보기 2153
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2153
이 정책 사용 2153
정책 세부 정보 2154
정책 버전 2154
JSON 정책 문서 2154
자세히 알아보기 2159
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2159
이 정책 사용 2159
정책 세부 정보 2159
정책 버전 2160
JSON 정책 문서 2160
자세히 알아보기 2161

AWSMigrationHubRefactorSpacesFullAccess 2161
이 정책 사용 2162
정책 세부 정보 2162
정책 버전 2162
JSON 정책 문서 2162
자세히 알아보기 2168
AWSMigrationHubRefactorSpacesServiceRolePolicy 2168
이 정책 사용 2168
정책 세부 정보 2168
정책 버전 2169
JSON 정책 문서 2169
자세히 알아보기 2173
AWSMigrationHubSMSAccess 2173
이 정책 사용 2173
정책 세부 정보 2173
정책 버전 2173
JSON 정책 문서 2173
자세히 알아보기 2174
AWSMigrationHubStrategyCollector 2175
이 정책 사용 2175
정책 세부 정보 2175
정책 버전 2175
JSON 정책 문서 2175
자세히 알아보기 2177
AWSMigrationHubStrategyConsoleFullAccess 2178
이 정책 사용 2178
정책 세부 정보 2178
정책 버전 2178
JSON 정책 문서 2178
자세히 알아보기 2180
AWSMigrationHubStrategyServiceRolePolicy 2180
이 정책 사용 2180
정책 세부 정보 2180
정책 버전 2181
JSON 정책 문서 2181
자세히 알아보기 2182

AWSMobileHub_FullAccess 2182
이 정책 사용 2182
정책 세부 정보 2182
정책 버전 2182
JSON 정책 문서 2182
자세히 알아보기 2184
AWSMobileHub_ReadOnly 2184
이 정책 사용 2184
정책 세부 정보 2184
정책 버전 2185
JSON 정책 문서 2185
자세히 알아보기 2186
AWSMSKReplicatorExecutionRole 2186
이 정책 사용 2186
정책 세부 정보 2186
정책 버전 2187
JSON 정책 문서 2187
자세히 알아보기 2188
AWSNetworkFirewallServiceRolePolicy 2188
이 정책 사용 2188
정책 세부 정보 2189
정책 버전 2189
JSON 정책 문서 2189
자세히 알아보기 2191
AWSNetworkManagerCloudWANServiceRolePolicy 2191
이 정책 사용 2191
정책 세부 정보 2191
정책 버전 2191
JSON 정책 문서 2191
자세히 알아보기 2192
AWSNetworkManagerFullAccess 2192
이 정책 사용 2192
정책 세부 정보 2192
정책 버전 2192
JSON 정책 문서 2193
자세히 알아보기 2193

AWSNetworkManagerReadOnlyAccess 2194
이 정책 사용 2194
정책 세부 정보 2194
정책 버전 2194
JSON 정책 문서 2194
자세히 알아보기 2195
AWSNetworkManagerServiceRolePolicy 2195
이 정책 사용 2195
정책 세부 정보 2195
정책 버전 2195
JSON 정책 문서 2196
자세히 알아보기 2197
AWSOpsWorks_FullAccess 2197
이 정책 사용 2197
정책 세부 정보 2197
정책 버전 2197
JSON 정책 문서 2197
자세히 알아보기 2198
AWSOpsWorksCloudWatchLogs 2199
이 정책 사용 2199
정책 세부 정보 2199
정책 버전 2199
JSON 정책 문서 2199
자세히 알아보기 2200
AWSOpsWorksCMInstanceProfileRole 2200
이 정책 사용 2200
정책 세부 정보 2200
정책 버전 2200
JSON 정책 문서 2201
자세히 알아보기 2202
AWSOpsWorksCMServiceRole 2202
이 정책 사용 2202
정책 세부 정보 2202
정책 버전 2202
JSON 정책 문서 2202
자세히 알아보기 2207

AWSOpsWorksInstanceRegistration 2207
이 정책 사용 2207
정책 세부 정보 2207
정책 버전 2207
JSON 정책 문서 2207
자세히 알아보기 2208
AWSOpsWorksRegisterCLI_EC2 2208
이 정책 사용 2208
정책 세부 정보 2208
정책 버전 2209
JSON 정책 문서 2209
자세히 알아보기 2210
AWSOpsWorksRegisterCLI_OnPremises 2210
이 정책 사용 2210
정책 세부 정보 2210
정책 버전 2210
JSON 정책 문서 2210
자세히 알아보기 2212
AWSOrganizationsFullAccess 2212
이 정책 사용 2212
정책 세부 정보 2212
정책 버전 2213
JSON 정책 문서 2213
자세히 알아보기 2214
AWSOrganizationsReadOnlyAccess 2214
이 정책 사용 2214
정책 세부 정보 2214
정책 버전 2214
JSON 정책 문서 2215
자세히 알아보기 2215
AWSOrganizationsServiceTrustPolicy 2215
이 정책 사용 2216
정책 세부 정보 2216
정책 버전 2216
JSON 정책 문서 2216
자세히 알아보기 2217

AWSOutpostsAuthorizeServerPolicy 2217
이 정책 사용 2217
정책 세부 정보 2217
정책 버전 2217
JSON 정책 문서 2218
자세히 알아보기 2218
AWSOutpostsServiceRolePolicy 2218
이 정책 사용 2218
정책 세부 정보 2218
정책 버전 2219
JSON 정책 문서 2219
자세히 알아보기 2219
AWSPanoramaApplianceRolePolicy 2219
이 정책 사용 2220
정책 세부 정보 2220
정책 버전 2220
JSON 정책 문서 2220
자세히 알아보기 2221
AWSPanoramaApplianceServiceRolePolicy 2221
이 정책 사용 2221
정책 세부 정보 2221
정책 버전 2221
JSON 정책 문서 2222
자세히 알아보기 2223
AWSPanoramaFullAccess 2223
이 정책 사용 2223
정책 세부 정보 2223
정책 버전 2224
JSON 정책 문서 2224
자세히 알아보기 2226
AWSPanoramaGreengrassGroupRolePolicy 2226
이 정책 사용 2227
정책 세부 정보 2227
정책 버전 2227
JSON 정책 문서 2227
자세히 알아보기 2228

AWSPanoramaSageMakerRolePolicy 2229
이 정책 사용 2229
정책 세부 정보 2229
정책 버전 2229
JSON 정책 문서 2229
자세히 알아보기 2230
AWSPanoramaServiceLinkedRolePolicy 2230
이 정책 사용 2230
정책 세부 정보 2230
정책 버전 2230
JSON 정책 문서 2231
자세히 알아보기 2233
AWSPanoramaServiceRolePolicy 2233
이 정책 사용 2233
정책 세부 정보 2234
정책 버전 2234
JSON 정책 문서 2234
자세히 알아보기 2241
AWSPriceListServiceFullAccess 2241
이 정책 사용 2241
정책 세부 정보 2241
정책 버전 2242
JSON 정책 문서 2242
자세히 알아보기 2242
AWSPrivateCAAuditor 2242
이 정책 사용 2242
정책 세부 정보 2243
정책 버전 2243
JSON 정책 문서 2243
자세히 알아보기 2244
AWSPrivateCAFullAccess 2244
이 정책 사용 2244
정책 세부 정보 2244
정책 버전 2244
JSON 정책 문서 2245
자세히 알아보기 2245

AWSPrivateCAPrivilegedUser 2245
이 정책 사용 2245
정책 세부 정보 2245
정책 버전 2246
JSON 정책 문서 2246
자세히 알아보기 2247
AWSPrivateCAReadOnly 2247
이 정책 사용 2247
정책 세부 정보 2247
정책 버전 2248
JSON 정책 문서 2248
자세히 알아보기 2248
AWSPrivateCAUser 2249
이 정책 사용 2249
정책 세부 정보 2249
정책 버전 2249
JSON 정책 문서 2249
자세히 알아보기 2250
AWSPrivateMarketplaceAdminFullAccess 2251
이 정책 사용 2251
정책 세부 정보 2251
정책 버전 2251
JSON 정책 문서 2251
자세히 알아보기 2253
AWSPrivateMarketplaceRequests 2253
이 정책 사용 2253
정책 세부 정보 2253
정책 버전 2253
JSON 정책 문서 2253
자세히 알아보기 2254
AWSPrivateNetworksServiceRolePolicy 2254
이 정책 사용 2254
정책 세부 정보 2254
정책 버전 2255
JSON 정책 문서 2255
자세히 알아보기 2255

AWSProtonCodeBuildProvisioningBasicAccess 2255
이 정책 사용 2256
정책 세부 정보 2256
정책 버전 2256
JSON 정책 문서 2256
자세히 알아보기 2257
AWSProtonCodeBuildProvisioningServiceRolePolicy 2257
이 정책 사용 2257
정책 세부 정보 2257
정책 버전 2257
JSON 정책 문서 2258
자세히 알아보기 2259
AWSProtonDeveloperAccess 2259
이 정책 사용 2259
정책 세부 정보 2259
정책 버전 2259
JSON 정책 문서 2260
자세히 알아보기 2262
AWSProtonFullAccess 2262
이 정책 사용 2262
정책 세부 정보 2262
정책 버전 2262
JSON 정책 문서 2262
자세히 알아보기 2264
AWSProtonReadOnlyAccess 2264
이 정책 사용 2264
정책 세부 정보 2264
정책 버전 2265
JSON 정책 문서 2265
자세히 알아보기 2266
AWSProtonServiceGitSyncServiceRolePolicy 2266
이 정책 사용 2266
정책 세부 정보 2267
정책 버전 2267
JSON 정책 문서 2267
자세히 알아보기 2268

AWSProtonSyncServiceRolePolicy 2268
이 정책 사용 2268
정책 세부 정보 2268
정책 버전 2268
JSON 정책 문서 2269
자세히 알아보기 2270
AWSPurchaseOrdersServiceRolePolicy 2270
이 정책 사용 2270
정책 세부 정보 2270
정책 버전 2270
JSON 정책 문서 2270
자세히 알아보기 2271
AWSQuicksightAthenaAccess 2271
이 정책 사용 2271
정책 세부 정보 2272
정책 버전 2272
JSON 정책 문서 2272
자세히 알아보기 2274
AWSQuickSightDescribeRDS 2274
이 정책 사용 2275
정책 세부 정보 2275
정책 버전 2275
JSON 정책 문서 2275
자세히 알아보기 2275
AWSQuickSightDescribeRedshift 2276
이 정책 사용 2276
정책 세부 정보 2276
정책 버전 2276
JSON 정책 문서 2276
자세히 알아보기 2277
AWSQuickSightElasticsearchPolicy 2277
이 정책 사용 2277
정책 세부 정보 2277
정책 버전 2277
JSON 정책 문서 2278
자세히 알아보기 2279

AWSQuickSightIoTAnalyticsAccess 2279
이 정책 사용 2279
정책 세부 정보 2279
정책 버전 2279
JSON 정책 문서 2279
자세히 알아보기 2280
AWSQuickSightListIAM 2280
이 정책 사용 2280
정책 세부 정보 2280
정책 버전 2281
JSON 정책 문서 2281
자세히 알아보기 2281
AWSQuicksightOpenSearchPolicy 2281
이 정책 사용 2281
정책 세부 정보 2282
정책 버전 2282
JSON 정책 문서 2282
자세히 알아보기 2283
AWSQuickSightSageMakerPolicy 2283
이 정책 사용 2283
정책 세부 정보 2283
정책 버전 2284
JSON 정책 문서 2284
자세히 알아보기 2285
AWSQuickSightTimestreamPolicy 2285
이 정책 사용 2285
정책 세부 정보 2286
정책 버전 2286
JSON 정책 문서 2286
자세히 알아보기 2287
AWSReachabilityAnalyzerServiceRolePolicy 2287
이 정책 사용 2287
정책 세부 정보 2287
정책 버전 2287
JSON 정책 문서 2287
자세히 알아보기 2290

AWSRefactoringToolkitFullAccess 2290
이 정책 사용 2290
정책 세부 정보 2290
정책 버전 2290
JSON 정책 문서 2291
자세히 알아보기 2304
AWSRefactoringToolkitSidecarPolicy 2304
이 정책 사용 2304
정책 세부 정보 2305
정책 버전 2305
JSON 정책 문서 2305
자세히 알아보기 2306
AWSrePostPrivateCloudWatchAccess 2306
이 정책 사용 2306
정책 세부 정보 2306
정책 버전 2307
JSON 정책 문서 2307
자세히 알아보기 2307
AWSRepostSpaceSupportOperationsPolicy 2308
이 정책 사용 2308
정책 세부 정보 2308
정책 버전 2308
JSON 정책 문서 2308
자세히 알아보기 2309
AWSResilienceHubAsssessmentExecutionPolicy 2309
이 정책 사용 2309
정책 세부 정보 2309
정책 버전 2309
JSON 정책 문서 2310
자세히 알아보기 2314
AWSResourceAccessManagerFullAccess 2314
이 정책 사용 2314
정책 세부 정보 2314
정책 버전 2314
JSON 정책 문서 2314
자세히 알아보기 2315

AWSResourceAccessManagerReadOnlyAccess 2315
이 정책 사용 2315
정책 세부 정보 2315
정책 버전 2315
JSON 정책 문서 2316
자세히 알아보기 2316
AWSResourceAccessManagerResourceShareParticipantAccess 2316
이 정책 사용 2316
정책 세부 정보 2317
정책 버전 2317
JSON 정책 문서 2317
자세히 알아보기 2318
AWSResourceAccessManagerServiceRolePolicy 2318
이 정책 사용 2318
정책 세부 정보 2318
정책 버전 2318
JSON 정책 문서 2318
자세히 알아보기 2319
AWSResourceExplorerFullAccess 2319
이 정책 사용 2320
정책 세부 정보 2320
정책 버전 2320
JSON 정책 문서 2320
자세히 알아보기 2321
AWSResourceExplorerOrganizationsAccess 2321
이 정책 사용 2321
정책 세부 정보 2321
정책 버전 2322
JSON 정책 문서 2322
자세히 알아보기 2323
AWSResourceExplorerReadOnlyAccess 2324
이 정책 사용 2324
정책 세부 정보 2324
정책 버전 2324
JSON 정책 문서 2324
자세히 알아보기 2325

AWSResourceExplorerServiceRolePolicy 2325
이 정책 사용 2325
정책 세부 정보 2325
정책 버전 2325
JSON 정책 문서 2326
자세히 알아보기 2335
AWSResourceGroupsReadOnlyAccess 2335
이 정책 사용 2335
정책 세부 정보 2335
정책 버전 2335
JSON 정책 문서 2335
자세히 알아보기 2337
AWSRoboMaker_FullAccess 2337
이 정책 사용 2337
정책 세부 정보 2337
정책 버전 2338
JSON 정책 문서 2338
자세히 알아보기 2339
AWSRoboMakerReadOnlyAccess 2339
이 정책 사용 2339
정책 세부 정보 2339
정책 버전 2340
JSON 정책 문서 2340
자세히 알아보기 2340
AWSRoboMakerServicePolicy 2340
이 정책 사용 2341
정책 세부 정보 2341
정책 버전 2341
JSON 정책 문서 2341
자세히 알아보기 2343
AWSRoboMakerServiceRolePolicy 2343
이 정책 사용 2343
정책 세부 정보 2343
정책 버전 2343
JSON 정책 문서 2343
자세히 알아보기 2345

AWSRolesAnywhereServicePolicy 2345
이 정책 사용 2345
정책 세부 정보 2345
정책 버전 2345
JSON 정책 문서 2345
자세히 알아보기 2346
AWSS3OnOutpostsServiceRolePolicy 2346
이 정책 사용 2347
정책 세부 정보 2347
정책 버전 2347
JSON 정책 문서 2347
자세히 알아보기 2350
AWSSavingsPlansFullAccess 2350
이 정책 사용 2350
정책 세부 정보 2350
정책 버전 2350
JSON 정책 문서 2350
자세히 알아보기 2351
AWSSavingsPlansReadOnlyAccess 2351
이 정책 사용 2351
정책 세부 정보 2351
정책 버전 2351
JSON 정책 문서 2352
자세히 알아보기 2352
AWSSecurityHubFullAccess 2352
이 정책 사용 2352
정책 세부 정보 2352
정책 버전 2353
JSON 정책 문서 2353
자세히 알아보기 2354
AWSSecurityHubOrganizationsAccess 2354
이 정책 사용 2354
정책 세부 정보 2354
정책 버전 2354
JSON 정책 문서 2355
자세히 알아보기 2356

AWSSecurityHubReadOnlyAccess 2356
이 정책 사용 2356
정책 세부 정보 2356
정책 버전 2356
JSON 정책 문서 2357
자세히 알아보기 2357
AWSSecurityHubServiceRolePolicy 2357
이 정책 사용 2357
정책 세부 정보 2357
정책 버전 2358
JSON 정책 문서 2358
자세히 알아보기 2360
AWSServiceCatalogAdminFullAccess 2360
이 정책 사용 2360
정책 세부 정보 2360
정책 버전 2360
JSON 정책 문서 2361
자세히 알아보기 2363
AWSServiceCatalogAdminReadOnlyAccess 2364
이 정책 사용 2364
정책 세부 정보 2364
정책 버전 2364
JSON 정책 문서 2364
자세히 알아보기 2365
AWSServiceCatalogAppRegistryFullAccess 2366
이 정책 사용 2366
정책 세부 정보 2366
정책 버전 2366
JSON 정책 문서 2366
자세히 알아보기 2368
AWSServiceCatalogAppRegistryReadOnlyAccess 2369
이 정책 사용 2369
정책 세부 정보 2369
정책 버전 2369
JSON 정책 문서 2369
자세히 알아보기 2370

AWSServiceCatalogAppRegistryServiceRolePolicy 2370
이 정책 사용 2370
정책 세부 정보 2370
정책 버전 2371
JSON 정책 문서 2371
자세히 알아보기 2372
AWSServiceCatalogEndUserFullAccess 2372
이 정책 사용 2372
정책 세부 정보 2372
정책 버전 2373
JSON 정책 문서 2373
자세히 알아보기 2375
AWSServiceCatalogEndUserReadOnlyAccess 2375
이 정책 사용 2375
정책 세부 정보 2375
정책 버전 2375
JSON 정책 문서 2376
자세히 알아보기 2377
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 2377
이 정책 사용 2378
정책 세부 정보 2378
정책 버전 2378
JSON 정책 문서 2378
자세히 알아보기 2379
AWSServiceCatalogSyncServiceRolePolicy 2379
이 정책 사용 2379
정책 세부 정보 2379
정책 버전 2379
JSON 정책 문서 2379
자세히 알아보기 2380
AWSServiceRoleForAmazonEKSNodegroup 2381
이 정책 사용 2381
정책 세부 정보 2381
정책 버전 2381
JSON 정책 문서 2381
자세히 알아보기 2385

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 2385
이 정책 사용 2386
정책 세부 정보 2386
정책 버전 2386
JSON 정책 문서 2386
자세히 알아보기 2386
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 2387
이 정책 사용 2387
정책 세부 정보 2387
정책 버전 2387
JSON 정책 문서 2387
자세히 알아보기 2388
AWSServiceRoleForCodeGuru-Profiler 2388
이 정책 사용 2388
정책 세부 정보 2388
정책 버전 2388
JSON 정책 문서 2389
자세히 알아보기 2389
AWSServiceRoleForCodeWhispererPolicy 2389
이 정책 사용 2389
정책 세부 정보 2390
정책 버전 2390
JSON 정책 문서 2390
자세히 알아보기 2392
AWSServiceRoleForEC2ScheduledInstances 2392
이 정책 사용 2392
정책 세부 정보 2392
정책 버전 2392
JSON 정책 문서 2393
자세히 알아보기 2393
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 2394
이 정책 사용 2394
정책 세부 정보 2394
정책 버전 2394
JSON 정책 문서 2394
자세히 알아보기 2395

AWSServiceRoleForImageBuilder 2395
이 정책 사용 2395
정책 세부 정보 2395
정책 버전 2395
JSON 정책 문서 2396
자세히 알아보기 2405
AWSServiceRoleForIoTSiteWise 2405
이 정책 사용 2405
정책 세부 정보 2406
정책 버전 2406
JSON 정책 문서 2406
자세히 알아보기 2407
AWSServiceRoleForLogDeliveryPolicy 2407
이 정책 사용 2408
정책 세부 정보 2408
정책 버전 2408
JSON 정책 문서 2408
자세히 알아보기 2409
AWSServiceRoleForMonitronPolicy 2409
이 정책 사용 2409
정책 세부 정보 2409
정책 버전 2409
JSON 정책 문서 2409
자세히 알아보기 2410
AWSServiceRoleForNeptuneGraphPolicy 2410
이 정책 사용 2410
정책 세부 정보 2410
정책 버전 2411
JSON 정책 문서 2411
자세히 알아보기 2412
AWSServiceRoleForPrivateMarketplaceAdminPolicy 2412
이 정책 사용 2412
정책 세부 정보 2413
정책 버전 2413
JSON 정책 문서 2413
자세히 알아보기 2415

AWSServiceRoleForSMS 2415
이 정책 사용 2415
정책 세부 정보 2415
정책 버전 2415
JSON 정책 문서 2415
자세히 알아보기 2422
AWSServiceRolePolicyForBackupReports 2422
이 정책 사용 2422
정책 세부 정보 2422
정책 버전 2423
JSON 정책 문서 2423
자세히 알아보기 2424
AWSServiceRolePolicyForBackupRestoreTesting 2424
이 정책 사용 2424
정책 세부 정보 2424
정책 버전 2425
JSON 정책 문서 2425
자세히 알아보기 2428
AWSShieldDRTAccessPolicy 2428
이 정책 사용 2428
정책 세부 정보 2428
정책 버전 2428
JSON 정책 문서 2428
자세히 알아보기 2429
AWSShieldServiceRolePolicy 2430
이 정책 사용 2430
정책 세부 정보 2430
정책 버전 2430
JSON 정책 문서 2430
자세히 알아보기 2431
AWSSSMForSAPServiceLinkedRolePolicy 2431
이 정책 사용 2431
정책 세부 정보 2431
정책 버전 2431
JSON 정책 문서 2432
자세히 알아보기 2438

AWSSSMOpsInsightsServiceRolePolicy 2438
이 정책 사용 2438
정책 세부 정보 2438
정책 버전 2438
JSON 정책 문서 2438
자세히 알아보기 2439
AWSSSODirectoryAdministrator 2439
이 정책 사용 2439
정책 세부 정보 2440
정책 버전 2440
JSON 정책 문서 2440
자세히 알아보기 2440
AWSSSODirectoryReadOnly 2441
이 정책 사용 2441
정책 세부 정보 2441
정책 버전 2441
JSON 정책 문서 2441
자세히 알아보기 2442
AWSSSOMasterAccountAdministrator 2442
이 정책 사용 2442
정책 세부 정보 2442
정책 버전 2443
JSON 정책 문서 2443
자세히 알아보기 2444
AWSSSOMemberAccountAdministrator 2445
이 정책 사용 2445
정책 세부 정보 2445
정책 버전 2445
JSON 정책 문서 2445
자세히 알아보기 2446
AWSSSOReadOnly 2447
이 정책 사용 2447
정책 세부 정보 2447
정책 버전 2447
JSON 정책 문서 2447
자세히 알아보기 2448

AWSSSOServiceRolePolicy 2448
이 정책 사용 2448
정책 세부 정보 2448
정책 버전 2449
JSON 정책 문서 2449
자세히 알아보기 2452
AWSStepFunctionsConsoleFullAccess 2453
이 정책 사용 2453
정책 세부 정보 2453
정책 버전 2453
JSON 정책 문서 2453
자세히 알아보기 2454
AWSStepFunctionsFullAccess 2454
이 정책 사용 2454
정책 세부 정보 2454
정책 버전 2455
JSON 정책 문서 2455
자세히 알아보기 2455
AWSStepFunctionsReadOnlyAccess 2455
이 정책 사용 2455
정책 세부 정보 2456
정책 버전 2456
JSON 정책 문서 2456
자세히 알아보기 2456
AWSStorageGatewayFullAccess 2457
이 정책 사용 2457
정책 세부 정보 2457
정책 버전 2457
JSON 정책 문서 2457
자세히 알아보기 2458
AWSStorageGatewayReadOnlyAccess 2458
이 정책 사용 2458
정책 세부 정보 2458
정책 버전 2459
JSON 정책 문서 2459
자세히 알아보기 2460

AWSStorageGatewayServiceRolePolicy 2460
이 정책 사용 2460
정책 세부 정보 2460
정책 버전 2460
JSON 정책 문서 2460
자세히 알아보기 2461
AWSSupplyChainFederationAdminAccess 2461
이 정책 사용 2461
정책 세부 정보 2461
정책 버전 2462
JSON 정책 문서 2462
자세히 알아보기 2467
AWSSupportAccess 2467
이 정책 사용 2467
정책 세부 정보 2467
정책 버전 2468
JSON 정책 문서 2468
자세히 알아보기 2468
AWSSupportAppFullAccess 2468
이 정책 사용 2469
정책 세부 정보 2469
정책 버전 2469
JSON 정책 문서 2469
자세히 알아보기 2470
AWSSupportAppReadOnlyAccess 2470
이 정책 사용 2470
정책 세부 정보 2470
정책 버전 2471
JSON 정책 문서 2471
자세히 알아보기 2471
AWSSupportPlansFullAccess 2471
이 정책 사용 2471
정책 세부 정보 2472
정책 버전 2472
JSON 정책 문서 2472
자세히 알아보기 2472

AWSSupportPlansReadOnlyAccess 2473
이 정책 사용 2473
정책 세부 정보 2473
정책 버전 2473
JSON 정책 문서 2473
자세히 알아보기 2474
AWSSupportServiceRolePolicy 2474
이 정책 사용 2474
정책 세부 정보 2474
정책 버전 2474
JSON 정책 문서 2475
자세히 알아보기 2548
AWSSystemsManagerAccountDiscoveryServicePolicy 2548
이 정책 사용 2548
정책 세부 정보 2549
정책 버전 2549
JSON 정책 문서 2549
자세히 알아보기 2550
AWSSystemsManagerChangeManagementServicePolicy 2550
이 정책 사용 2550
정책 세부 정보 2550
정책 버전 2550
JSON 정책 문서 2550
자세히 알아보기 2552
AWSSystemsManagerForSAPFullAccess 2552
이 정책 사용 2552
정책 세부 정보 2552
정책 버전 2553
JSON 정책 문서 2553
자세히 알아보기 2554
AWSSystemsManagerForSAPReadOnlyAccess 2554
이 정책 사용 2554
정책 세부 정보 2554
정책 버전 2554
JSON 정책 문서 2554
자세히 알아보기 2555

AWSSystemsManagerOpsDataSyncServiceRolePolicy 2555
이 정책 사용 2555
정책 세부 정보 2555
정책 버전 2556
JSON 정책 문서 2556
자세히 알아보기 2559
AWSThinkboxAssetServerPolicy 2560
이 정책 사용 2560
정책 세부 정보 2560
정책 버전 2560
JSON 정책 문서 2560
자세히 알아보기 2561
AWSThinkboxAWSPortalAdminPolicy 2561
이 정책 사용 2561
정책 세부 정보 2561
정책 버전 2562
JSON 정책 문서 2562
자세히 알아보기 2571
AWSThinkboxAWSPortalGatewayPolicy 2572
이 정책 사용 2572
정책 세부 정보 2572
정책 버전 2572
JSON 정책 문서 2572
자세히 알아보기 2574
AWSThinkboxAWSPortalWorkerPolicy 2574
이 정책 사용 2574
정책 세부 정보 2574
정책 버전 2575
JSON 정책 문서 2575
자세히 알아보기 2577
AWSThinkboxDeadlineResourceTrackerAccessPolicy 2577
이 정책 사용 2577
정책 세부 정보 2577
정책 버전 2577
JSON 정책 문서 2578
자세히 알아보기 2580

AWSThinkboxDeadlineResourceTrackerAdminPolicy 2581
이 정책 사용 2581
정책 세부 정보 2581
정책 버전 2581
JSON 정책 문서 2581
자세히 알아보기 2587
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 2587
이 정책 사용 2587
정책 세부 정보 2587
정책 버전 2587
JSON 정책 문서 2588
자세히 알아보기 2590
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 2591
이 정책 사용 2591
정책 세부 정보 2591
정책 버전 2591
JSON 정책 문서 2591
자세히 알아보기 2593
AWSTransferConsoleFullAccess 2593
이 정책 사용 2593
정책 세부 정보 2593
정책 버전 2593
JSON 정책 문서 2593
자세히 알아보기 2594
AWSTransferFullAccess 2595
이 정책 사용 2595
정책 세부 정보 2595
정책 버전 2595
JSON 정책 문서 2595
자세히 알아보기 2596
AWSTransferLoggingAccess 2596
이 정책 사용 2596
정책 세부 정보 2596
정책 버전 2597
JSON 정책 문서 2597
자세히 알아보기 2597

AWSTransferReadOnlyAccess 2597
이 정책 사용 2598
정책 세부 정보 2598
정책 버전 2598
JSON 정책 문서 2598
자세히 알아보기 2599
AWSTrustedAdvisorPriorityFullAccess 2599
이 정책 사용 2599
정책 세부 정보 2599
정책 버전 2599
JSON 정책 문서 2599
자세히 알아보기 2601
AWSTrustedAdvisorPriorityReadOnlyAccess 2601
이 정책 사용 2602
정책 세부 정보 2602
정책 버전 2602
JSON 정책 문서 2602
자세히 알아보기 2603
AWSTrustedAdvisorReportingServiceRolePolicy 2603
이 정책 사용 2603
정책 세부 정보 2603
정책 버전 2604
JSON 정책 문서 2604
자세히 알아보기 2604
AWSTrustedAdvisorServiceRolePolicy 2605
이 정책 사용 2605
정책 세부 정보 2605
정책 버전 2605
JSON 정책 문서 2605
자세히 알아보기 2608
AWSUserNotificationsServiceLinkedRolePolicy 2608
이 정책 사용 2608
정책 세부 정보 2608
정책 버전 2608
JSON 정책 문서 2609
자세히 알아보기 2609

AWSVendorInsightsAssessorFullAccess 2610
이 정책 사용 2610
정책 세부 정보 2610
정책 버전 2610
JSON 정책 문서 2610
자세히 알아보기 2611
AWSVendorInsightsAssessorReadOnly 2612
이 정책 사용 2612
정책 세부 정보 2612
정책 버전 2612
JSON 정책 문서 2612
자세히 알아보기 2613
AWSVendorInsightsVendorFullAccess 2613
이 정책 사용 2613
정책 세부 정보 2613
정책 버전 2613
JSON 정책 문서 2614
자세히 알아보기 2615
AWSVendorInsightsVendorReadOnly 2616
이 정책 사용 2616
정책 세부 정보 2616
정책 버전 2616
JSON 정책 문서 2616
자세히 알아보기 2617
AWSVpcLatticeServiceRolePolicy 2617
이 정책 사용 2618
정책 세부 정보 2618
정책 버전 2618
JSON 정책 문서 2618
자세히 알아보기 2619
AWSVPCS2SVpnServiceRolePolicy 2619
이 정책 사용 2619
정책 세부 정보 2619
정책 버전 2619
JSON 정책 문서 2619
자세히 알아보기 2620

AWSVPCTransitGatewayServiceRolePolicy 2620
이 정책 사용 2620
정책 세부 정보 2620
정책 버전 2620
JSON 정책 문서 2621
자세히 알아보기 2621
AWSVPCVerifiedAccessServiceRolePolicy 2621
이 정책 사용 2621
정책 세부 정보 2622
정책 버전 2622
JSON 정책 문서 2622
자세히 알아보기 2624
AWSWAFConsoleFullAccess 2624
이 정책 사용 2624
정책 세부 정보 2624
정책 버전 2624
JSON 정책 문서 2624
자세히 알아보기 2626
AWSWAFConsoleReadOnlyAccess 2627
이 정책 사용 2627
정책 세부 정보 2627
정책 버전 2627
JSON 정책 문서 2627
자세히 알아보기 2628
AWSWAFFullAccess 2628
이 정책 사용 2629
정책 세부 정보 2629
정책 버전 2629
JSON 정책 문서 2629
자세히 알아보기 2631
AWSWAFReadOnlyAccess 2631
이 정책 사용 2631
정책 세부 정보 2631
정책 버전 2631
JSON 정책 문서 2632
자세히 알아보기 2632

AWSWellArchitectedDiscoveryServiceRolePolicy 2633
이 정책 사용 2633
정책 세부 정보 2633
정책 버전 2633
JSON 정책 문서 2633
자세히 알아보기 2635
AWSWellArchitectedOrganizationsServiceRolePolicy 2635
이 정책 사용 2635
정책 세부 정보 2635
정책 버전 2635
JSON 정책 문서 2636
자세히 알아보기 2636
AWSWickrFullAccess 2636
이 정책 사용 2636
정책 세부 정보 2636
정책 버전 2637
JSON 정책 문서 2637
자세히 알아보기 2637
AWSXrayCrossAccountSharingConfiguration 2637
이 정책 사용 2638
정책 세부 정보 2638
정책 버전 2638
JSON 정책 문서 2638
자세히 알아보기 2639
AWSXRayDaemonWriteAccess 2639
이 정책 사용 2639
정책 세부 정보 2639
정책 버전 2640
JSON 정책 문서 2640
자세히 알아보기 2640
AWSXrayFullAccess 2641
이 정책 사용 2641
정책 세부 정보 2641
정책 버전 2641
JSON 정책 문서 2641
자세히 알아보기 2642

AWSXrayReadOnlyAccess 2642
이 정책 사용 2642
정책 세부 정보 2642
정책 버전 2642
JSON 정책 문서 2642
자세히 알아보기 2643
AWSXrayWriteOnlyAccess 2643
이 정책 사용 2644
정책 세부 정보 2644
정책 버전 2644
JSON 정책 문서 2644
자세히 알아보기 2645
AWSZonalAutoshiftPracticeRunSLRPolicy 2645
이 정책 사용 2645
정책 세부 정보 2645
정책 버전 2645
JSON 정책 문서 2645
자세히 알아보기 2646
BatchServiceRolePolicy 2646
이 정책 사용 2646
정책 세부 정보 2647
정책 버전 2647
JSON 정책 문서 2647
자세히 알아보기 2653
Billing 2653
이 정책 사용 2653
정책 세부 정보 2653
정책 버전 2654
JSON 정책 문서 2654
자세히 알아보기 2656
CertificateManagerServiceRolePolicy 2657
이 정책 사용 2657
정책 세부 정보 2657
정책 버전 2657
JSON 정책 문서 2657
자세히 알아보기 2658

ClientVPNServiceConnectionsRolePolicy 2658
이 정책 사용 2658
정책 세부 정보 2658
정책 버전 2658
JSON 정책 문서 2658
자세히 알아보기 2659
ClientVPNServiceRolePolicy 2659
이 정책 사용 2659
정책 세부 정보 2659
정책 버전 2659
JSON 정책 문서 2660
자세히 알아보기 2660
CloudFormationStackSetsOrgAdminServiceRolePolicy 2661
이 정책 사용 2661
정책 세부 정보 2661
정책 버전 2661
JSON 정책 문서 2661
자세히 알아보기 2662
CloudFormationStackSetsOrgMemberServiceRolePolicy 2662
이 정책 사용 2662
정책 세부 정보 2662
정책 버전 2662
JSON 정책 문서 2663
자세히 알아보기 2663
CloudFrontFullAccess 2664
이 정책 사용 2664
정책 세부 정보 2664
정책 버전 2664
JSON 정책 문서 2664
자세히 알아보기 2665
CloudFrontReadOnlyAccess 2666
이 정책 사용 2666
정책 세부 정보 2666
정책 버전 2666
JSON 정책 문서 2666
자세히 알아보기 2667

CloudHSMServiceRolePolicy 2667
이 정책 사용 2667
정책 세부 정보 2667
정책 버전 2668
JSON 정책 문서 2668
자세히 알아보기 2668
CloudSearchFullAccess 2668
이 정책 사용 2669
정책 세부 정보 2669
정책 버전 2669
JSON 정책 문서 2669
자세히 알아보기 2669
CloudSearchReadOnlyAccess 2670
이 정책 사용 2670
정책 세부 정보 2670
정책 버전 2670
JSON 정책 문서 2670
자세히 알아보기 2671
CloudTrailServiceRolePolicy 2671
이 정책 사용 2671
정책 세부 정보 2671
정책 버전 2671
JSON 정책 문서 2672
자세히 알아보기 2673
CloudWatch-CrossAccountAccess 2673
이 정책 사용 2673
정책 세부 정보 2674
정책 버전 2674
JSON 정책 문서 2674
자세히 알아보기 2674
CloudWatchActionsEC2Access 2675
이 정책 사용 2675
정책 세부 정보 2675
정책 버전 2675
JSON 정책 문서 2675
자세히 알아보기 2676

CloudWatchAgentAdminPolicy 2676
이 정책 사용 2676
정책 세부 정보 2676
정책 버전 2676
JSON 정책 문서 2677
자세히 알아보기 2677
CloudWatchAgentServerPolicy 2678
이 정책 사용 2678
정책 세부 정보 2678
정책 버전 2678
JSON 정책 문서 2678
자세히 알아보기 2679
CloudWatchApplicationInsightsFullAccess 2679
이 정책 사용 2679
정책 세부 정보 2680
정책 버전 2680
JSON 정책 문서 2680
자세히 알아보기 2681
CloudWatchApplicationInsightsReadOnlyAccess 2682
이 정책 사용 2682
정책 세부 정보 2682
정책 버전 2682
JSON 정책 문서 2682
자세히 알아보기 2683
CloudwatchApplicationInsightsServiceLinkedRolePolicy 2683
이 정책 사용 2683
정책 세부 정보 2683
정책 버전 2683
JSON 정책 문서 2684
자세히 알아보기 2693
CloudWatchApplicationSignalsServiceRolePolicy 2693
이 정책 사용 2694
정책 세부 정보 2694
정책 버전 2694
JSON 정책 문서 2694
자세히 알아보기 2696

CloudWatchAutomaticDashboardsAccess 2696
이 정책 사용 2696
정책 세부 정보 2696
정책 버전 2696
JSON 정책 문서 2697
자세히 알아보기 2698
CloudWatchCrossAccountSharingConfiguration 2698
이 정책 사용 2698
정책 세부 정보 2698
정책 버전 2699
JSON 정책 문서 2699
자세히 알아보기 2700
CloudWatchEventsBuiltInTargetExecutionAccess 2700
이 정책 사용 2700
정책 세부 정보 2700
정책 버전 2700
JSON 정책 문서 2701
자세히 알아보기 2701
CloudWatchEventsFullAccess 2701
이 정책 사용 2701
정책 세부 정보 2701
정책 버전 2702
JSON 정책 문서 2702
자세히 알아보기 2704
CloudWatchEventsInvocationAccess 2704
이 정책 사용 2704
정책 세부 정보 2704
정책 버전 2704
JSON 정책 문서 2705
자세히 알아보기 2705
CloudWatchEventsReadOnlyAccess 2705
이 정책 사용 2705
정책 세부 정보 2705
정책 버전 2706
JSON 정책 문서 2706
자세히 알아보기 2707

CloudWatchEventsServiceRolePolicy 2707
이 정책 사용 2708
정책 세부 정보 2708
정책 버전 2708
JSON 정책 문서 2708
자세히 알아보기 2709
CloudWatchFullAccess 2709
이 정책 사용 2709
정책 세부 정보 2709
정책 버전 2709
JSON 정책 문서 2709
자세히 알아보기 2710
CloudWatchFullAccessV2 2711
이 정책 사용 2711
정책 세부 정보 2711
정책 버전 2711
JSON 정책 문서 2711
자세히 알아보기 2713
CloudWatchInternetMonitorServiceRolePolicy 2713
이 정책 사용 2713
정책 세부 정보 2713
정책 버전 2713
JSON 정책 문서 2714
자세히 알아보기 2715
CloudWatchLambdaInsightsExecutionRolePolicy 2715
이 정책 사용 2715
정책 세부 정보 2715
정책 버전 2715
JSON 정책 문서 2715
자세히 알아보기 2716
CloudWatchLogsCrossAccountSharingConfiguration 2716
이 정책 사용 2716
정책 세부 정보 2716
정책 버전 2717
JSON 정책 문서 2717
자세히 알아보기 2718

CloudWatchLogsFullAccess 2718
이 정책 사용 2718
정책 세부 정보 2718
정책 버전 2718
JSON 정책 문서 2719
자세히 알아보기 2719
CloudWatchLogsReadOnlyAccess 2719
이 정책 사용 2719
정책 세부 정보 2719
정책 버전 2720
JSON 정책 문서 2720
자세히 알아보기 2720
CloudWatchNetworkMonitorServiceRolePolicy 2721
이 정책 사용 2721
정책 세부 정보 2721
정책 버전 2721
JSON 정책 문서 2721
자세히 알아보기 2723
CloudWatchReadOnlyAccess 2723
이 정책 사용 2723
정책 세부 정보 2723
정책 버전 2723
JSON 정책 문서 2723
자세히 알아보기 2725
CloudWatchSyntheticsFullAccess 2725
이 정책 사용 2725
정책 세부 정보 2725
정책 버전 2725
JSON 정책 문서 2725
자세히 알아보기 2730
CloudWatchSyntheticsReadOnlyAccess 2730
이 정책 사용 2730
정책 세부 정보 2730
정책 버전 2731
JSON 정책 문서 2731
자세히 알아보기 2731

ComprehendDataAccessRolePolicy 2731
이 정책 사용 2732
정책 세부 정보 2732
정책 버전 2732
JSON 정책 문서 2732
자세히 알아보기 2733
ComprehendFullAccess 2733
이 정책 사용 2733
정책 세부 정보 2733
정책 버전 2733
JSON 정책 문서 2733
자세히 알아보기 2734
ComprehendMedicalFullAccess 2734
이 정책 사용 2734
정책 세부 정보 2734
정책 버전 2735
JSON 정책 문서 2735
자세히 알아보기 2735
ComprehendReadOnly 2735
이 정책 사용 2735
정책 세부 정보 2736
정책 버전 2736
JSON 정책 문서 2736
자세히 알아보기 2737
ComputeOptimizerReadOnlyAccess 2737
이 정책 사용 2738
정책 세부 정보 2738
정책 버전 2738
JSON 정책 문서 2738
자세히 알아보기 2739
ComputeOptimizerServiceRolePolicy 2739
이 정책 사용 2739
정책 세부 정보 2739
정책 버전 2740
JSON 정책 문서 2740
자세히 알아보기 2741

ConfigConformsServiceRolePolicy 2741
이 정책 사용 2741
정책 세부 정보 2742
정책 버전 2742
JSON 정책 문서 2742
자세히 알아보기 2745
CostOptimizationHubAdminAccess 2745
이 정책 사용 2745
정책 세부 정보 2745
정책 버전 2745
JSON 정책 문서 2746
자세히 알아보기 2747
CostOptimizationHubReadOnlyAccess 2747
이 정책 사용 2747
정책 세부 정보 2747
정책 버전 2747
JSON 정책 문서 2748
자세히 알아보기 2748
CostOptimizationHubServiceRolePolicy 2748
이 정책 사용 2749
정책 세부 정보 2749
정책 버전 2749
JSON 정책 문서 2749
자세히 알아보기 2750
CustomerProfilesServiceLinkedRolePolicy 2750
이 정책 사용 2750
정책 세부 정보 2750
정책 버전 2751
JSON 정책 문서 2751
자세히 알아보기 2751
DatabaseAdministrator 2752
이 정책 사용 2752
정책 세부 정보 2752
정책 버전 2752
JSON 정책 문서 2752
자세히 알아보기 2755

DataScientist 2755
이 정책 사용 2755
정책 세부 정보 2755
정책 버전 2755
JSON 정책 문서 2755
자세히 알아보기 2759
DAXServiceRolePolicy 2759
이 정책 사용 2759
정책 세부 정보 2760
정책 버전 2760
JSON 정책 문서 2760
자세히 알아보기 2761
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 2761
이 정책 사용 2761
정책 세부 정보 2761
정책 버전 2761
JSON 정책 문서 2761
자세히 알아보기 2762
DynamoDBKinesisReplicationServiceRolePolicy 2762
이 정책 사용 2762
정책 세부 정보 2762
정책 버전 2763
JSON 정책 문서 2763
자세히 알아보기 2763
DynamoDBReplicationServiceRolePolicy 2764
이 정책 사용 2764
정책 세부 정보 2764
정책 버전 2764
JSON 정책 문서 2764
자세히 알아보기 2765
EC2FastLaunchServiceRolePolicy 2766
이 정책 사용 2766
정책 세부 정보 2766
정책 버전 2766
JSON 정책 문서 2766
자세히 알아보기 2770

EC2FleetTimeShiftableServiceRolePolicy 2770
이 정책 사용 2770
정책 세부 정보 2770
정책 버전 2771
JSON 정책 문서 2771
자세히 알아보기 2772
Ec2ImageBuilderCrossAccountDistributionAccess 2772
이 정책 사용 2773
정책 세부 정보 2773
정책 버전 2773
JSON 정책 문서 2773
자세히 알아보기 2774
EC2ImageBuilderLifecycleExecutionPolicy 2774
이 정책 사용 2774
정책 세부 정보 2774
정책 버전 2774
JSON 정책 문서 2775
자세히 알아보기 2776
EC2InstanceConnect 2777
이 정책 사용 2777
정책 세부 정보 2777
정책 버전 2777
JSON 정책 문서 2777
자세히 알아보기 2778
Ec2InstanceConnectEndpoint 2778
이 정책 사용 2778
정책 세부 정보 2778
정책 버전 2778
JSON 정책 문서 2779
자세히 알아보기 2781
EC2InstanceProfileForImageBuilder 2781
이 정책 사용 2781
정책 세부 정보 2781
정책 버전 2781
JSON 정책 문서 2781
자세히 알아보기 2782

EC2InstanceProfileForImageBuilderECRContainerBuilds 2783
이 정책 사용 2783
정책 세부 정보 2783
정책 버전 2783
JSON 정책 문서 2783
자세히 알아보기 2785
ECRReplicationServiceRolePolicy 2785
이 정책 사용 2785
정책 세부 정보 2785
정책 버전 2785
JSON 정책 문서 2786
자세히 알아보기 2786
ElastiCacheServiceRolePolicy 2786
이 정책 사용 2786
정책 세부 정보 2786
정책 버전 2787
JSON 정책 문서 2787
자세히 알아보기 2789
ElasticLoadBalancingFullAccess 2789
이 정책 사용 2789
정책 세부 정보 2789
정책 버전 2789
JSON 정책 문서 2789
자세히 알아보기 2791
ElasticLoadBalancingReadOnly 2791
이 정책 사용 2791
정책 세부 정보 2791
정책 버전 2791
JSON 정책 문서 2792
자세히 알아보기 2793
ElementalActivationsDownloadSoftwareAccess 2793
이 정책 사용 2793
정책 세부 정보 2793
정책 버전 2793
JSON 정책 문서 2794
자세히 알아보기 2794

ElementalActivationsFullAccess 2794
이 정책 사용 2794
정책 세부 정보 2794
정책 버전 2795
JSON 정책 문서 2795
자세히 알아보기 2795
ElementalActivationsGenerateLicenses 2795
이 정책 사용 2795
정책 세부 정보 2796
정책 버전 2796
JSON 정책 문서 2796
자세히 알아보기 2796
ElementalActivationsReadOnlyAccess 2797
이 정책 사용 2797
정책 세부 정보 2797
정책 버전 2797
JSON 정책 문서 2797
자세히 알아보기 2798
ElementalAppliancesSoftwareFullAccess 2798
이 정책 사용 2798
정책 세부 정보 2798
정책 버전 2798
JSON 정책 문서 2798
자세히 알아보기 2799
ElementalAppliancesSoftwareReadOnlyAccess 2799
이 정책 사용 2799
정책 세부 정보 2799
정책 버전 2800
JSON 정책 문서 2800
자세히 알아보기 2800
ElementalSupportCenterFullAccess 2800
이 정책 사용 2800
정책 세부 정보 2801
정책 버전 2801
JSON 정책 문서 2801
자세히 알아보기 2801

EMRDescribeClusterPolicyForEMRWAL 2802
이 정책 사용 2802
정책 세부 정보 2802
정책 버전 2802
JSON 정책 문서 2802
자세히 알아보기 2803
FMSServiceRolePolicy 2803
이 정책 사용 2803
정책 세부 정보 2803
정책 버전 2803
JSON 정책 문서 2803
자세히 알아보기 2817
FSxDeleteServiceLinkedRoleAccess 2818
이 정책 사용 2818
정책 세부 정보 2818
정책 버전 2818
JSON 정책 문서 2818
자세히 알아보기 2819
GameLiftGameServerGroupPolicy 2819
이 정책 사용 2819
정책 세부 정보 2819
정책 버전 2819
JSON 정책 문서 2819
자세히 알아보기 2821
GlobalAcceleratorFullAccess 2821
이 정책 사용 2821
정책 세부 정보 2821
정책 버전 2822
JSON 정책 문서 2822
자세히 알아보기 2823
GlobalAcceleratorReadOnlyAccess 2823
이 정책 사용 2823
정책 세부 정보 2823
정책 버전 2823
JSON 정책 문서 2824
자세히 알아보기 2824

GreengrassOTAUpdateArtifactAccess 2824
이 정책 사용 2824
정책 세부 정보 2824
정책 버전 2825
JSON 정책 문서 2825
자세히 알아보기 2825
GroundTruthSyntheticConsoleFullAccess 2826
이 정책 사용 2826
정책 세부 정보 2826
정책 버전 2826
JSON 정책 문서 2826
자세히 알아보기 2827
GroundTruthSyntheticConsoleReadOnlyAccess 2827
이 정책 사용 2827
정책 세부 정보 2827
정책 버전 2827
JSON 정책 문서 2827
자세히 알아보기 2828
Health_OrganizationsServiceRolePolicy 2828
이 정책 사용 2828
정책 세부 정보 2828
정책 버전 2829
JSON 정책 문서 2829
자세히 알아보기 2829
IAMAccessAdvisorReadOnly 2829
이 정책 사용 2830
정책 세부 정보 2830
정책 버전 2830
JSON 정책 문서 2830
자세히 알아보기 2831
IAMAccessAnalyzerFullAccess 2831
이 정책 사용 2831
정책 세부 정보 2831
정책 버전 2832
JSON 정책 문서 2832
자세히 알아보기 2833

IAMAccessAnalyzerReadOnlyAccess 2833
이 정책 사용 2833
정책 세부 정보 2833
정책 버전 2833
JSON 정책 문서 2834
자세히 알아보기 2834
IAMFullAccess 2834
이 정책 사용 2834
정책 세부 정보 2835
정책 버전 2835
JSON 정책 문서 2835
자세히 알아보기 2836
IAMReadOnlyAccess 2836
이 정책 사용 2836
정책 세부 정보 2836
정책 버전 2836
JSON 정책 문서 2836
자세히 알아보기 2837
IAMSelfManageServiceSpecificCredentials 2837
이 정책 사용 2837
정책 세부 정보 2837
정책 버전 2838
JSON 정책 문서 2838
자세히 알아보기 2838
IAMUserChangePassword 2838
이 정책 사용 2839
정책 세부 정보 2839
정책 버전 2839
JSON 정책 문서 2839
자세히 알아보기 2840
IAMUserSSHKeys 2840
이 정책 사용 2840
정책 세부 정보 2840
정책 버전 2840
JSON 정책 문서 2840
자세히 알아보기 2841

IVSFullAccess 2841
이 정책 사용 2841
정책 세부 정보 2841
정책 버전 2842
JSON 정책 문서 2842
자세히 알아보기 2842
IVSReadOnlyAccess 2842
이 정책 사용 2843
정책 세부 정보 2843
정책 버전 2843
JSON 정책 문서 2843
자세히 알아보기 2844
IVSRecordToS3 2844
이 정책 사용 2844
정책 세부 정보 2845
정책 버전 2845
JSON 정책 문서 2845
자세히 알아보기 2845
KafkaConnectServiceRolePolicy 2846
이 정책 사용 2846
정책 세부 정보 2846
정책 버전 2846
JSON 정책 문서 2846
자세히 알아보기 2848
KafkaServiceRolePolicy 2848
이 정책 사용 2848
정책 세부 정보 2848
정책 버전 2848
JSON 정책 문서 2848
자세히 알아보기 2850
KeyspacesReplicationServiceRolePolicy 2850
이 정책 사용 2850
정책 세부 정보 2850
정책 버전 2851
JSON 정책 문서 2851
자세히 알아보기 2851

LakeFormationDataAccessServiceRolePolicy 2851
이 정책 사용 2851
정책 세부 정보 2852
정책 버전 2852
JSON 정책 문서 2852
자세히 알아보기 2852
LexBotPolicy 2853
이 정책 사용 2853
정책 세부 정보 2853
정책 버전 2853
JSON 정책 문서 2853
자세히 알아보기 2854
LexChannelPolicy 2854
이 정책 사용 2854
정책 세부 정보 2854
정책 버전 2854
JSON 정책 문서 2855
자세히 알아보기 2855
LightsailExportAccess 2855
이 정책 사용 2855
정책 세부 정보 2855
정책 버전 2856
JSON 정책 문서 2856
자세히 알아보기 2857
MediaConnectGatewayInstanceRolePolicy 2857
이 정책 사용 2857
정책 세부 정보 2857
정책 버전 2857
JSON 정책 문서 2857
자세히 알아보기 2858
MediaPackageServiceRolePolicy 2858
이 정책 사용 2858
정책 세부 정보 2858
정책 버전 2858
JSON 정책 문서 2859
자세히 알아보기 2859

MemoryDBServiceRolePolicy 2859
이 정책 사용 2860
정책 세부 정보 2860
정책 버전 2860
JSON 정책 문서 2860
자세히 알아보기 2862
MigrationHubDMSAccessServiceRolePolicy 2862
이 정책 사용 2862
정책 세부 정보 2862
정책 버전 2863
JSON 정책 문서 2863
자세히 알아보기 2864
MigrationHubServiceRolePolicy 2864
이 정책 사용 2864
정책 세부 정보 2864
정책 버전 2864
JSON 정책 문서 2864
자세히 알아보기 2866
MigrationHubSMSAccessServiceRolePolicy 2866
이 정책 사용 2866
정책 세부 정보 2866
정책 버전 2866
JSON 정책 문서 2867
자세히 알아보기 2867
MonitronServiceRolePolicy 2868
이 정책 사용 2868
정책 세부 정보 2868
정책 버전 2868
JSON 정책 문서 2868
자세히 알아보기 2869
NeptuneConsoleFullAccess 2869
이 정책 사용 2869
정책 세부 정보 2869
정책 버전 2869
JSON 정책 문서 2870
자세히 알아보기 2875

NeptuneFullAccess 2875
이 정책 사용 2875
정책 세부 정보 2876
정책 버전 2876
JSON 정책 문서 2876
자세히 알아보기 2880
NeptuneGraphReadOnlyAccess 2880
이 정책 사용 2880
정책 세부 정보 2880
정책 버전 2880
JSON 정책 문서 2881
자세히 알아보기 2882
NeptuneReadOnlyAccess 2882
이 정책 사용 2882
정책 세부 정보 2883
정책 버전 2883
JSON 정책 문서 2883
자세히 알아보기 2885
NetworkAdministrator 2885
이 정책 사용 2885
정책 세부 정보 2886
정책 버전 2886
JSON 정책 문서 2886
자세히 알아보기 2892
OAMFullAccess 2893
이 정책 사용 2893
정책 세부 정보 2893
정책 버전 2893
JSON 정책 문서 2893
자세히 알아보기 2894
OAMReadOnlyAccess 2894
이 정책 사용 2894
정책 세부 정보 2894
정책 버전 2894
JSON 정책 문서 2895
자세히 알아보기 2895

PartnerCentralAccountManagementUserRoleAssociation 2895
이 정책 사용 2895
정책 세부 정보 2895
정책 버전 2896
JSON 정책 문서 2896
자세히 알아보기 2897
PowerUserAccess 2897
이 정책 사용 2897
정책 세부 정보 2897
정책 버전 2897
JSON 정책 문서 2897
자세히 알아보기 2898
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 2898
이 정책 사용 2898
정책 세부 정보 2899
정책 버전 2899
JSON 정책 문서 2899
자세히 알아보기 2900
RDSCloudHsmAuthorizationRole 2900
이 정책 사용 2900
정책 세부 정보 2900
정책 버전 2900
JSON 정책 문서 2900
자세히 알아보기 2901
ReadOnlyAccess 2901
이 정책 사용 2901
정책 세부 정보 2901
정책 버전 2902
JSON 정책 문서 2902
자세히 알아보기 2948
ResourceGroupsandTagEditorFullAccess 2948
이 정책 사용 2948
정책 세부 정보 2948
정책 버전 2949
JSON 정책 문서 2949
자세히 알아보기 2949

ResourceGroupsandTagEditorReadOnlyAccess 2950
이 정책 사용 2950
정책 세부 정보 2950
정책 버전 2950
JSON 정책 문서 2950
자세히 알아보기 2951
ResourceGroupsServiceRolePolicy 2951
이 정책 사용 2951
정책 세부 정보 2951
정책 버전 2951
JSON 정책 문서 2952
자세히 알아보기 2952
ROSAAmazonEBSCSIDriverOperatorPolicy 2952
이 정책 사용 2952
정책 세부 정보 2953
정책 버전 2953
JSON 정책 문서 2953
자세히 알아보기 2956
ROSACloudNetworkConfigOperatorPolicy 2956
이 정책 사용 2956
정책 세부 정보 2956
정책 버전 2957
JSON 정책 문서 2957
자세히 알아보기 2958
ROSAControlPlaneOperatorPolicy 2958
이 정책 사용 2958
정책 세부 정보 2958
정책 버전 2958
JSON 정책 문서 2959
자세히 알아보기 2963
ROSAImageRegistryOperatorPolicy 2963
이 정책 사용 2963
정책 세부 정보 2964
정책 버전 2964
JSON 정책 문서 2964
자세히 알아보기 2965

ROSAIngressOperatorPolicy 2965
이 정책 사용 2966
정책 세부 정보 2966
정책 버전 2966
JSON 정책 문서 2966
자세히 알아보기 2967
ROSAInstallerPolicy 2967
이 정책 사용 2967
정책 세부 정보 2967
정책 버전 2968
JSON 정책 문서 2968
자세히 알아보기 2975
ROSAKMSProviderPolicy 2975
이 정책 사용 2975
정책 세부 정보 2975
정책 버전 2976
JSON 정책 문서 2976
자세히 알아보기 2976
ROSAKubeControllerPolicy 2977
이 정책 사용 2977
정책 세부 정보 2977
정책 버전 2977
JSON 정책 문서 2977
자세히 알아보기 2982
ROSAManageSubscription 2982
이 정책 사용 2982
정책 세부 정보 2982
정책 버전 2982
JSON 정책 문서 2982
자세히 알아보기 2983
ROSANodePoolManagementPolicy 2983
이 정책 사용 2984
정책 세부 정보 2984
정책 버전 2984
JSON 정책 문서 2984
자세히 알아보기 2990

ROSASRESupportPolicy 2990
이 정책 사용 2990
정책 세부 정보 2990
정책 버전 2990
JSON 정책 문서 2991
자세히 알아보기 2995
ROSAWorkerInstancePolicy 2996
이 정책 사용 2996
정책 세부 정보 2996
정책 버전 2996
JSON 정책 문서 2996
자세히 알아보기 2997
Route53RecoveryReadinessServiceRolePolicy 2997
이 정책 사용 2997
정책 세부 정보 2997
정책 버전 2997
JSON 정책 문서 2998
자세히 알아보기 3001
Route53ResolverServiceRolePolicy 3001
이 정책 사용 3001
정책 세부 정보 3001
정책 버전 3002
JSON 정책 문서 3002
자세히 알아보기 3002
S3StorageLensServiceRolePolicy 3003
이 정책 사용 3003
정책 세부 정보 3003
정책 버전 3003
JSON 정책 문서 3003
자세히 알아보기 3004
SecretsManagerReadWrite 3004
이 정책 사용 3004
정책 세부 정보 3004
정책 버전 3004
JSON 정책 문서 3005
자세히 알아보기 3006

SecurityAudit 3006
이 정책 사용 3006
정책 세부 정보 3007
정책 버전 3007
JSON 정책 문서 3007
자세히 알아보기 3023
SecurityLakeServiceLinkedRole 3023
이 정책 사용 3023
정책 세부 정보 3023
정책 버전 3023
JSON 정책 문서 3023
자세히 알아보기 3026
ServerMigration_ServiceRole 3026
이 정책 사용 3026
정책 세부 정보 3026
정책 버전 3027
JSON 정책 문서 3027
자세히 알아보기 3031
ServerMigrationConnector 3032
이 정책 사용 3032
정책 세부 정보 3032
정책 버전 3032
JSON 정책 문서 3032
자세히 알아보기 3034
ServerMigrationServiceConsoleFullAccess 3034
이 정책 사용 3034
정책 세부 정보 3034
정책 버전 3034
JSON 정책 문서 3035
자세히 알아보기 3036
ServerMigrationServiceLaunchRole 3037
이 정책 사용 3037
정책 세부 정보 3037
정책 버전 3037
JSON 정책 문서 3037
자세히 알아보기 3040

ServerMigrationServiceRoleForInstanceValidation 3040
이 정책 사용 3040
정책 세부 정보 3040
정책 버전 3041
JSON 정책 문서 3041
자세히 알아보기 3041
ServiceQuotasFullAccess 3042
이 정책 사용 3042
정책 세부 정보 3042
정책 버전 3042
JSON 정책 문서 3042
자세히 알아보기 3044
ServiceQuotasReadOnlyAccess 3044
이 정책 사용 3044
정책 세부 정보 3044
정책 버전 3044
JSON 정책 문서 3045
자세히 알아보기 3046
ServiceQuotasServiceRolePolicy 3046
이 정책 사용 3046
정책 세부 정보 3046
정책 버전 3046
JSON 정책 문서 3047
자세히 알아보기 3047
SimpleWorkflowFullAccess 3047
이 정책 사용 3047
정책 세부 정보 3047
정책 버전 3048
JSON 정책 문서 3048
자세히 알아보기 3048
SupportUser 3048
이 정책 사용 3048
정책 세부 정보 3049
정책 버전 3049
JSON 정책 문서 3049
자세히 알아보기 3054

SystemAdministrator 3054
이 정책 사용 3054
정책 세부 정보 3054
정책 버전 3055
JSON 정책 문서 3055
자세히 알아보기 3061
TranslateFullAccess 3061
이 정책 사용 3061
정책 세부 정보 3061
정책 버전 3061
JSON 정책 문서 3062
자세히 알아보기 3062
TranslateReadOnly 3062
이 정책 사용 3062
정책 세부 정보 3063
정책 버전 3063
JSON 정책 문서 3063
자세히 알아보기 3064
ViewOnlyAccess 3064
이 정책 사용 3064
정책 세부 정보 3064
정책 버전 3064
JSON 정책 문서 3064
자세히 알아보기 3070
VMImportExportRoleForAWSConnector 3070
이 정책 사용 3071
정책 세부 정보 3071
정책 버전 3071
JSON 정책 문서 3071
자세히 알아보기 3072
VPCLatticeFullAccess 3072
이 정책 사용 3072
정책 세부 정보 3072
정책 버전 3072
JSON 정책 문서 3073
자세히 알아보기 3075

VPCLatticeReadOnlyAccess 3075
이 정책 사용 3075
정책 세부 정보 3075
정책 버전 3075
JSON 정책 문서 3075
자세히 알아보기 3076
VPCLatticeServicesInvokeAccess 3076
이 정책 사용 3077
정책 세부 정보 3077
정책 버전 3077
JSON 정책 문서 3077
자세히 알아보기 3077
WAFLoggingServiceRolePolicy 3078
이 정책 사용 3078
정책 세부 정보 3078
정책 버전 3078
JSON 정책 문서 3078
자세히 알아보기 3079
WAFRegionalLoggingServiceRolePolicy 3079
이 정책 사용 3079
정책 세부 정보 3079
정책 버전 3079
JSON 정책 문서 3080
자세히 알아보기 3080
WAFV2LoggingServiceRolePolicy 3080
이 정책 사용 3080
정책 세부 정보 3080
정책 버전 3081
JSON 정책 문서 3081
자세히 알아보기 3081
WellArchitectedConsoleFullAccess 3082
이 정책 사용 3082
정책 세부 정보 3082
정책 버전 3082
JSON 정책 문서 3082
자세히 알아보기 3083

WellArchitectedConsoleReadOnlyAccess 3083
이 정책 사용 3083
정책 세부 정보 3083
정책 버전 3083
JSON 정책 문서 3083
자세히 알아보기 3084
WorkLinkServiceRolePolicy 3084
이 정책 사용 3084
정책 세부 정보 3084
정책 버전 3084
JSON 정책 문서 3085
자세히 알아보기 3085
..... mmmlxxxvi

AWS 관리형 정책이란 무엇인가요?

AWS 관리형 정책은 AWS에 의해 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다. 이를 사용하면 직접 정책을 작성하는 경우보다는 사용자, 그룹 및 역할에 권한 할당을 시작하는 것이 더욱 쉽습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

정책 참조 페이지 이해

각 정책 참조 페이지에는 다음 정보가 포함됩니다.

- 이 정책 사용 - 사용자, 그룹, 역할에 정책을 연결할 수 있는지 여부
- 정책 세부 정보
  - 유형 - AWS 관리형 정책 유형
    - `AWS managed policy` - 표준 AWS 관리형 정책
    - `Job function policy` - 업계 공통 직무 기능에 부합하는 정책
    - `Service-linked role policy` - 서비스가 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결된 정책(예: the section called “AmazonRDSPreviewServiceRolePolicy”)
    - `Service role policy` - 서비스 역할과 연계되도록 설계된 정책(예: the section called “AWSControlTowerServiceRolePolicy”)
  - 생성 시간 - 정책이 처음 생성된 시점
  - 편집된 시간 - 이 버전의 정책이 편집된 시점
  - ARN - 정책의 Amazon 리소스 이름(ARN)
- 정책 버전 - 정책에 의해 부여된 권한의 버전
- JSON 정책 문서 - 정책 JSON

- 자세히 알아보기 - AWS 관리형 정책과 관련된 설명서 링크

사용되지 않는 AWS 관리형 정책

AWS는 AWS 관리형 정책을 정기적으로 업데이트합니다. 대부분의 경우, 정책에 권한을 추가합니다. 이는 새 서비스나 기능을 출시할 때 발생합니다. AWS 관리형 정책의 보안을 개선하기 위해 때때로 정책 범위를 축소합니다. 정책에서 권한을 제거할 때는 정책을 사용 중단 상태로 설정하고 새 정책을 사용할 수 있도록 만듭니다. AWS가 서비스 또는 기능을 더 이상 사용하지 않는 경우 해당 기능에 대한 AWS 관리형 정책도 더 이상 사용되지 않습니다.

사용 중인 정책이 더 이상 사용되지 않는다는 이메일 알림을 받으면 즉시 조치를 취하는 것이 좋습니다. 정책 변경 사항을 파악하고 워크플로를 업데이트하세요. AWS가 대체 정책을 제공하는 경우 영향을 받는 모든 자격 증명(사용자, 그룹 및 역할)에 이를 연결한 다음 해당 자격 증명에서 더 이상 사용되지 않는 정책을 분리할 계획입니다.

사용되지 않는 정책은 다음과 같은 특성을 갖습니다.

- 이 안내서에서는 삭제되었습니다.
- 권한은 현재 연결된 모든 자격 증명에 대해 계속 작동합니다.
- 정책이 자격 증명에 연결된 계정에서는 IAM 콘솔의 정책 목록에 경고 아이콘과 함께 표시됩니다.
- 새 자격 증명에는 연결할 수 없습니다. 현재 자격 증명에서 연결을 해제할 경우 다시 연결할 수 없습니다.
- 현재의 모든 엔터티로부터 연결을 해제하면 더 이상 표시되지 않습니다.

AWS 관리형 정책

AWS 관리형 정책

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy

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

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

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

- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess

- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess

- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForSMS
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess

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

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

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

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

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

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

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

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

AccessAnalyzerServiceRolePolicy

`AccessAnalyzerServiceRolePolicy`는 AWS 관리형 정책으로, Access Analyzer가 리소스 메타데이터를 분석할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 2일, 17:13 UTC
- 편집 시간: 2024년 1월 22일 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AdministratorAccess

`AdministratorAccess` AWS 서비스 및 리소스에 대한 전체 액세스 권한을 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AdministratorAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AdministratorAccess-Amplify

`AdministratorAccess-Amplify`는 AWS 관리형 정책으로, Amplify 애플리케이션에 필요한 리소스에 대한 직접 액세스를 명시적으로 허용하면서 계정 관리 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AdministratorAccess-Amplify`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 19:03 UTC
- 편집된 시간: 2023년 5월 31일, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

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

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

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

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

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

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

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AdministratorAccess-AWSElasticBeanstalk

`AdministratorAccess-AWSElasticBeanstalk`는 AWS 관리형 정책으로, 계정 관리 권한을 부여합니다. 개발자와 관리자가 AWS Elastic Beanstalk 애플리케이션을 관리하는 데 필요한 리소스에 직접 액세스할 수 있도록 명시적으로 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AdministratorAccess-AWSElasticBeanstalk`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 19:36 UTC
- 편집된 시간: 2023년 3월 23일, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

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

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

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

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

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessDeviceSetup

`AlexaForBusinessDeviceSetup`은 AWS 관리형 정책으로, AlexaForBusiness 서비스에 대한 디바이스 설정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessDeviceSetup`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2019년 5월 20일, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessFullAccess

`AlexaForBusinessFullAccess`는 AWS 관리형 정책으로, AlexaForBusiness 리소스에 대한 전체 액세스와 관련 AWS 서비스에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2020년 7월 1일, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessGatewayExecution

`AlexaForBusinessGatewayExecution`은 AWS 관리형 정책으로, AlexaForBusiness 서비스에 대한 게이이트웨이 실행 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessGatewayExecution`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2017년 11월 30일, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessLifesizeDelegatedAccessPolicy

`AlexaForBusinessLifesizeDelegatedAccessPolicy`는 AWS 관리형 정책으로, Lifesize AVS 디바이스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessLifesizeDelegatedAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 4일, 19:46 UTC
- 편집된 시간: 2020년 6월 12일, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessNetworkProfileServicePolicy

`AlexaForBusinessNetworkProfileServicePolicy`는 AWS 관리형 정책으로, 이 정책은 Alexa for Business가 네트워크 프로필에서 예약된 자동화 태스크를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 3월 13일, 00:53 UTC
- 편집된 시간: 2019년 4월 5일, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessPolyDelegatedAccessPolicy

`AlexaForBusinessPolyDelegatedAccessPolicy`는 AWS 관리형 정책으로, Poly AVS 디바이스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AlexaForBusinessPolyDelegatedAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 16일, 19:48 UTC
- 편집된 시간: 2019년 10월 16일, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AlexaForBusinessReadOnlyAccess

`AlexaForBusinessReadOnlyAccess`은 AWS 관리형 정책으로, AlexaForBusiness 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AlexaForBusinessReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:47 UTC
- 편집된 시간: 2019년 11월 20일, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAPIGatewayAdministrator

`AmazonAPIGatewayAdministrator`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon API Gateway에서 API를 생성/편집/삭제할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAPIGatewayAdministrator`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:34 UTC
- 편집된 시간: 2015년 7월 9일, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAPIGatewayInvokeFullAccess

AmazonAPIGatewayInvokeFullAccess는 AWS 관리형 정책으로, Amazon API Gateway에서 API를 호출할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAPIGatewayInvokeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:36 UTC
- 편집된 시간: 2018년 12월 18일, 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogs는 AWS 관리형 정책으로, API Gateway가 사용자의 계정에 로그를 푸시할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAPIGatewayPushToCloudWatchLogs를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 11일, 23:41 UTC
- 편집된 시간: 2015년 11월 11일, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppFlowFullAccess

`AmazonAppFlowFullAccess`는 AWS 관리형 정책으로, Amazon AppFlow에 대한 전체 액세스와 흐름 소스 또는 대상(S3 및 Redshift)으로 지원되는 AWS 서비스에 대한 액세스를 제공합니다. 또한 암호화를 위해 KMS에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAppFlowFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 2일, 23:30 UTC
- 편집된 시간: 2022년 2월 28일, 23:11 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppFlowReadOnlyAccess

`AmazonAppFlowReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Appflow 흐름에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAppFlowReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 2일, 23:26 UTC
- 편집된 시간: 2022년 2월 28일, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppStreamFullAccess

`AmazonAppStreamFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon AppStream에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAppStreamFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 8월 28일, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppStreamPCAAccess

`AmazonAppStreamPCAAccess`는 AWS 관리형 정책으로, 인증서 기반 인증을 위한 고객 계정의 AWS Certificate Manager Private CA에 대한 Amazon AppStream 2.0 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAppStreamPCAAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 24일, 17:05 UTC
- 편집된 시간: 2022년 10월 24일, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppStreamReadOnlyAccess

`AmazonAppStreamReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon AppStream에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAppStreamReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 12월 7일, 21:00 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAppStreamServiceAccess

`AmazonAppStreamServiceAccess`는 AWS 관리형 정책으로, Amazon AppStream 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAppStreamServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 19일, 04:17 UTC
- 편집된 시간: 2020년 6월 26일, 16:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAthenaFullAccess

`AmazonAthenaFullAccess`는 AWS 관리형 정책으로, Amazon Athena에 대한 전체 액세스 권한과 쿼리, 결과 작성 및 데이터 관리를 활성화하는 데 필요한 종속성에 대한 범위 지정된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAthenaFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 16:46 UTC
- 편집 시간: 2024년 1월 3일 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAugmentedAIFullAccess

AmazonAugmentedAIFullAccess는 AWS 관리형 정책으로, FlowDefinitions, HumanTaskUis, HumanLoops를 포함한 모든 작업 Amazon Augmented AI 리소스를 수행할 수 있는 액세스를 제공합니다. 퍼블릭 크라우드 Workteam에 대해 FlowDefinitions를 생성할 수 있는 액세스를 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAugmentedAIFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:21 UTC
- 편집된 시간: 2019년 12월 3일, 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess는 AWS 관리형 정책으로, HumanLoops에서 모든 작업을 수행할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonAugmentedAIHumanLoopFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:20 UTC
- 편집된 시간: 2019년 12월 3일, 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonAugmentedAIIntegratedAPIAccess

`AmazonAugmentedAIIntegratedAPIAccess`는 AWS 관리형 정책으로, FlowDefinitions, HumanTaskUis, HumanLoops를 포함한 모든 작업 Amazon Augmented AI 리소스를 수행할 수 있는 액세스를 제공합니다. 또한 Amazon Augmented AI와 통합된 서비스 운영에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonAugmentedAIIntegratedAPIAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 22일, 20:47 UTC
- 편집된 시간: 2020년 4월 22일, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonBedrockFullAccess

`AmazonBedrockFullAccess`Amazon Bedrock에 대한 전체 액세스 권한과 필요한 관련 서비스에 대한 제한된 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonBedrockFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 12월 6일, 15:47 UTC
- 편집 시간: 2023년 12월 6일, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonBedrockReadOnly

`AmazonBedrockReadOnly`Amazon Bedrock에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonBedrockReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 12월 6일, 15:48 UTC
- 편집 시간: 2023년 12월 6일, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonBraketFullAccess

AmazonBraketFullAccess는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Amazon Braket에 대한 전체 액세스를 제공합니다. 또한 관련 서비스(예: S3, logs)에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBraketFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 6일, 20:12 UTC
- 편집된 시간: 2023년 4월 19일, 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
```

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

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicy는 AWS 관리형 정책으로, S3, Cloudwatch, IAM, Braket을 포함한 Amazon Braket Job을 실행하는 데 필요한 AWS 서비스 및 리소스에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonBraketJobsExecutionPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 26일, 19:34 UTC
- 편집된 시간: 2021년 11월 28일, 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonBraketServiceRolePolicy

`AmazonBraketServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Braket이 사용자를 대신하여 AWS 리소스를 생성 및 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 4일, 17:12 UTC
- 편집된 시간: 2020년 8월 6일, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeFullAccess

`AmazonChimeFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Chime Admin Console에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:15 UTC
- 편집된 시간: 2020년 12월 14일, 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeReadOnly

`AmazonChimeReadOnly`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Chime Admin Console에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonChimeReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:04 UTC
- 편집된 시간: 2020년 12월 14일, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeSDK

AmazonChimeSDK는 AWS 관리형 정책으로, Amazon Chime SDK 작업에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeSDK를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 4일, 21:53 UTC
- 편집된 시간: 2023년 1월 10일, 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy는 다음과 같은 AWS관리형 정책입니다. Amazon Chime SDK MediaPipelines 서비스 연결 역할에 대한 관리형 정책

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 4월 4일, 22:02 UTC
- 편집 시간: 2023년 12월 8일 19:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy는 AWS 관리형 정책으로, Amazon Chime SDK Messaging이 AWS 리소스에 액세스하고 메시징 기능을 활성화하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 3일, 01:43 UTC
- 편집된 시간: 2023년 3월 3일, 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy는 AWS 관리형 정책으로, Amazon Chime에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 9월 30일, 22:25 UTC
- 편집된 시간: 2019년 9월 30일, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy는 AWS 관리형 정책으로, Amazon Chime이 사용자를 대신하여 Amazon Transcribe 및 Amazon Transcribe Medical에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 4일, 21:47 UTC
- 편집된 시간: 2021년 8월 4일, 21:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeUserManagement

AmazonChimeUserManagement는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Chime Admin Console에 대한 사용자 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonChimeUserManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 1일, 22:17 UTC
- 편집된 시간: 2020년 2월 18일, 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Amazon Chime VoiceConnector의 서비스 연결 역할에 대한 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 9월 30일, 22:16 UTC
- 편집된 시간: 2023년 4월 14일, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess는 AWS 관리형 정책으로, Amazon Cloud Directory Service에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudDirectoryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 25일, 00:41 UTC
- 편집된 시간: 2017년 2월 25일, 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudDirectoryReadOnlyAccess

`AmazonCloudDirectoryReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Cloud Directory Service에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCloudDirectoryReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 28일, 23:42 UTC
- 편집된 시간: 2017년 2월 28일, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchEvidentlyFullAccess

`AmazonCloudWatchEvidentlyFullAccess`는 AWS 관리형 정책으로, Amazon CloudWatch Evidently에 대한 전체 액세스만 제공합니다. 또한 관련 Amazon S3, Amazon SNS, Amazon CloudWatch 및 기타 관련 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCloudWatchEvidentlyFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:10 UTC
- 편집된 시간: 2021년 11월 29일, 15:10 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchEvidentlyReadOnlyAccess

AmazonCloudWatchEvidentlyReadOnlyAccess는 AWS 관리형 정책으로, Amazon CloudWatch Evidently에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchEvidentlyReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:08 UTC
- 편집된 시간: 2021년 11월 29일, 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchEvidentlyServiceRolePolicy

`AmazonCloudWatchEvidentlyServiceRolePolicy`는 AWS 관리형 정책으로, CloudWatch Evidently Service가 고객을 대신하여 연관된 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 13일, 17:25 UTC
- 편집된 시간: 2022년 9월 13일, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchRUMFullAccess

AmazonCloudWatchRUMFullAccess는 AWS 관리형 정책으로, Amazon CloudWatch RUM 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchRUMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:46 UTC

- 편집된 시간: 2021년 11월 29일, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess는 AWS 관리형 정책으로, Amazon CloudWatch RUM 서비스에 대한 읽기 전용 액세스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCloudWatchRUMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 15:43 UTC
- 편집된 시간: 2022년 10월 28일, 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCloudWatchRUMServiceRolePolicy

`AmazonCloudWatchRUMServiceRolePolicy`는 AWS 관리형 정책으로, Amazon CloudWatch RUM 서비스에 모니터링 데이터를 다른 관련 AWS 서비스에 게시할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 23:17 UTC
- 편집된 시간: 2023년 2월 22일, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeCatalystFullAccess

`AmazonCodeCatalystFullAccess`는 AWS 관리형 정책으로, Amazon CodeCatalyst에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeCatalystFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 20일, 16:50 UTC
- 편집된 시간: 2023년 4월 20일, 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeCatalystReadOnlyAccess

`AmazonCodeCatalystReadOnlyAccess`는 AWS 관리형 정책으로, Amazon CodeCatalyst에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeCatalystReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 20일, 16:49 UTC
- 편집된 시간: 2023년 4월 20일, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeCatalystSupportAccess

`AmazonCodeCatalystSupportAccess`는 AWS 관리형 정책으로, Amazon CodeCatalyst가 사용자를 대신하여 AWS Support 사례를 생성, 업데이트 및 해결할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeCatalystSupportAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2023년 4월 20일, 12:34 UTC
- 편집된 시간: 2023년 4월 20일, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruProfilerAgentAccess

`AmazonCodeGuruProfilerAgentAccess`는 AWS 관리형 정책으로, Amazon CodeGuru Profiler 에이전트에 필요한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeGuruProfilerAgentAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 5일, 22:11 UTC
- 편집된 시간: 2022년 5월 5일, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruProfilerFullAccess

`AmazonCodeGuruProfilerFullAccess`는 AWS 관리형 정책으로, Amazon CodeGuru Profiler에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeGuruProfilerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 10:13 UTC
- 편집된 시간: 2020년 7월 15일, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruProfilerReadOnlyAccess

AmazonCodeGuruProfilerReadOnlyAccess는 AWS 관리형 정책으로, Amazon CodeGuru Profiler에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruProfilerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 10:30 UTC
- 편집된 시간: 2020년 6월 27일, 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruReviewerFullAccess

`AmazonCodeGuruReviewerFullAccess`는 AWS 관리형 정책으로, Amazon CodeGuru Reviewer에 대한 전체 액세스 권한과 필수 종속성에 대한 범위 지정된 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeGuruReviewerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 08:33 UTC
- 편집된 시간: 2020년 8월 29일, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruReviewerReadOnlyAccess

`AmazonCodeGuruReviewerReadOnlyAccess`는 AWS 관리형 정책으로, Amazon CodeGuru Reviewer에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruReviewerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 08:48 UTC
- 편집된 시간: 2020년 8월 29일, 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy는 AWS 관리형 정책으로, Amazon CodeGuru Reviewer가 사용자를 대신하여 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 3일, 05:31 UTC
- 편집된 시간: 2020년 11월 27일, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruSecurityFullAccess

AmazonCodeGuruSecurityFullAccess는 AWS 관리형 정책으로, Amazon CodeGuru Security에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCodeGuruSecurityFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 9일, 21:03 UTC
- 편집된 시간: 2023년 5월 9일, 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCodeGuruSecurityScanAccess

`AmazonCodeGuruSecurityScanAccess`는 AWS 관리형 정책으로, Amazon CodeGuru Security 검사 작업에 필요한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCodeGuruSecurityScanAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 9일, 20:54 UTC
- 편집된 시간: 2023년 5월 9일, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoDeveloperAuthenticatedIdentities

`AmazonCognitoDeveloperAuthenticatedIdentities`는 AWS 관리형 정책으로, 인증 백엔드에서 개발자 인증 자격 증명을 지원하기 위해 Amazon Cognito APIs에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCognitoDeveloperAuthenticatedIdentities`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:22 UTC
- 편집된 시간: 2015년 3월 24일, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoIdpEmailServiceRolePolicy

`AmazonCognitoIdpEmailServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Cognito User Pools 서비스가 이메일 전송에 SES 자격 증명을 사용할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 3월 21일, 21:32 UTC
- 편집된 시간: 2019년 3월 21일, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoIdpServiceRolePolicy

`AmazonCognitoIdpServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Cognito User Pools에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 26일, 22:30 UTC
- 편집된 시간: 2020년 6월 26일, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoPowerUser

`AmazonCognitoPowerUser`는 AWS 관리형 정책으로, 기존 Amazon Cognito 리소스에 대한 관리 액세스를 제공합니다. 새 Cognito 리소스를 생성하려면 AWS 계정 관리자 권한이 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCognitoPowerUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:14 UTC
- 편집된 시간: 2021년 6월 1일, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoReadOnly

AmazonCognitoReadOnly는 AWS 관리형 정책으로, Amazon Cognito에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 3월 24일, 17:06 UTC
- 편집된 시간: 2019년 8월 1일, 19:21 UTC

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

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoUnAuthedIdentitiesSessionPolicy

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`는 AWS 관리형 정책으로, 이 정책은 Cognito Identity Pools의 인증되지 않은 자격 증명에 허용되는 권한 세트를 정의합니다. 이 정책은 독립형 권한 정책으로 사용하기 위한 것이 아닙니다. 이는 자격 증명 풀의 역할에 연결된 지나치게 허용적인 정책을 막기 위한 가드레일로 사용됩니다. Cognito Identity Service는 자격 증명을 생성할 때 자동으로 범위 축소 정책으로 포함하므로 이 정책을 어떤 역할에도 연결하지 마십시오. 향상된 흐름을 통해 다른 AWS 리소스에 일시적으로 액세스할 수 있는 권한은 이제 서비스에서 제공하는 인증되지 않은 사용자의 자격 증명과 연관된 역할과 Cognito가 소유한 이 관리형 정책에 부여된 권한의 교집합에 의해 정의됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonCognitoUnAuthedIdentitiesSessionPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 19일, 23:04 UTC
- 편집된 시간: 2023년 7월 19일, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonCognitoUnauthenticatedIdentities

`AmazonCognitoUnauthenticatedIdentities`는 AWS 관리형 정책으로, 이 정책은 Cognito Identity Pools의 인증되지 않은 자격 증명에 허용되는 권한 세트를 정의합니다. Cognito Identity Service는 자격 증명을 생성할 때 자동으로 범위 축소 정책으로 포함하므로 이를 unauth 역할에 연결할 필요가 없습니다. 향상된 흐름을 통해 다른 AWS 리소스에 일시적으로 액세스할 수 있는 권한은 이제 서비스에서 제공하는 인증되지 않은 사용자의 자격 증명과 연관된 역할과 Cognito가 소유한 이 관리형 정책에 부여된 권한의 교집합에 의해 정의됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonCognitoUnauthenticatedIdentities를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 1일, 22:36 UTC
- 편집된 시간: 2023년 2월 1일, 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnect_FullAccess

AmazonConnect_FullAccess는 AWS 관리형 정책으로, 이 정책의 목적은 AWS Connect 사용자에게 Connect 리소스를 사용하는 데 필요한 권한을 부여하는 것입니다. 이 정책은 Connect Console 및 퍼블릭 API를 통해 AWS Connect 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonConnect_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 19:54 UTC
- 편집된 시간: 2023년 3월 7일, 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnectCampaignsServiceLinkedRolePolicy

`AmazonConnectCampaignsServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Amazon Connect Campaigns 서비스 연결 역할에 대한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 23일, 20:54 UTC
- 편집된 시간: 2023년 11월 8일, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnectReadOnlyAccess

`AmazonConnectReadOnlyAccess`는 AWS 관리형 정책으로, 사용자의 AWS 계정에서 Amazon Connect 인스턴스를 볼 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonConnectReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 17일, 21:00 UTC
- 편집된 시간: 2019년 11월 6일, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnectServiceLinkedRolePolicy

`AmazonConnectServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Amazon Connect가 사용자를 대신하여 AWS 리소스를 생성 및 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 9월 7일, 00:21 UTC
- 편집 시간: 2023년 11월 28일 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

```
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
```

```
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy는 AWS 관리형 정책으로, Amazon Connect가 사용자를 대신하여 리전 간에 AWS 리소스를 동기화할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2023년 10월 27일, 22:38 UTC
- 편집된 시간: 2023년 10월 27일, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect:DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect:DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",
        "connect:CreateAgentStatus",
        "connect:UpdateAgentStatus",
        "connect:DescribeAgentStatus",
        "connect:ListAgentStatuses",
        "connect:CreateQuickConnect",
        "connect:UpdateQuickConnect*",
        "connect:DeleteQuickConnect",
        "connect:DescribeQuickConnect",
        "connect:ListQuickConnects",
```

```
        "connect:CreateHoursOfOperation",
        "connect:UpdateHoursOfOperation",
        "connect:DeleteHoursOfOperation",
        "connect:DescribeHoursOfOperation",
        "connect:ListHoursOfOperations",
        "connect:CreateQueue",
        "connect:UpdateQueue*",
        "connect:DeleteQueue",
        "connect:DescribeQueue",
        "connect:ListQueue*",
        "connect:CreatePrompt",
        "connect:UpdatePrompt",
        "connect:DeletePrompt",
        "connect:DescribePrompt",
        "connect:ListPrompts",
        "connect:GetPromptFile",
        "connect:CreateSecurityProfile",
        "connect:UpdateSecurityProfile",
        "connect:DeleteSecurityProfile",
        "connect:DescribeSecurityProfile",
        "connect:ListSecurityProfile*",
        "connect:CreateContactFlow*",
        "connect:UpdateContactFlow*",
        "connect:DeleteContactFlow*",
        "connect:DescribeContactFlow*",
        "connect:ListContactFlow*",
        "connect:BatchGetFlowAssociation",
        "connect:CreatePredefinedAttribute",
        "connect:UpdatePredefinedAttribute",
        "connect:DeletePredefinedAttribute",
        "connect:DescribePredefinedAttribute",
        "connect:ListPredefinedAttributes",
        "connect:ListTagsForResource",
        "connect:TagResource",
        "connect:UntagResource",
        "connect:ListTrafficDistributionGroups",
        "connect:ListPhoneNumbersV2",
        "connect:UpdatePhoneNumber",
        "connect:DescribePhoneNumber",
        "connect:Associate*",
        "connect:Disassociate*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonConnectVoiceIDFullAccess

`AmazonConnectVoiceIDFullAccess`는 AWS 관리형 정책으로, Amazon Connect Voice ID에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonConnectVoiceIDFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 26일, 19:04 UTC
- 편집된 시간: 2021년 9월 26일, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZoneDomainExecutionRolePolicy

`AmazonDataZoneDomainExecutionRolePolicy` DataZoneAmazon의 DomainExecutionRole 서비스 역할에 대한 기본 정책인 AWS 관리형 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDataZoneDomainExecutionRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 9월 27일, 21:55 UTC

- 편집 시간: 2024년 3월 12일 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
```

```
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
```

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonDataZoneEnvironmentRolePermissionsBoundary

`AmazonDataZoneEnvironmentRolePermissionsBoundary`Amazon은 데이터 분석 작업을 수행하기 위해 Environments에 대한 IAM 역할을 DataZone 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한 범위를 정의하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDataZoneEnvironmentRolePermissionsBoundary`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 11일, 23:38 UTC
- 편집 시간: 2023년 11월 17일 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZoneFullAccess

AmazonDataZoneFullAccess는 다음과 AWS Management Console 같은 AWS 관리형 정책입니다. DataZone Amazon에 대한 전체 액세스 권한은 물론 필요한 관련 서비스에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 22일, 20:06 UTC
- 편집 시간: 2024년 3월 12일 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonDataZoneFullUserAccess

AmazonDataZoneFullUserAccessAmazon에 대한 전체 액세스를 제공하지만 도메인 DataZone, 사용자 또는 관련 계정의 관리는 허용하지 않는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneFullUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 22일, 21:06 UTC
- 편집 시간: 2024년 3월 12일 23:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
```

```
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
```

```
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
```

```
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonDataZoneGlueManageAccessRolePolicy

`AmazonDataZoneGlueManageAccessRolePolicy`다음과 같은 AWS관리형 정책입니다. 정책은 Amazon이 데이터에 대한 게시 및 액세스 권한을 DataZone 허용할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDataZoneGlueManageAccessRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 9월 22일, 20:21 UTC
- 편집 시간: 2023년 12월 14일 23:03 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTableDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
```

```
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
```

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy는 AWS 관리형 정책으로, Amazon DataZone API에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZonePortalFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 26일, 18:24 UTC
- 편집된 시간: 2023년 3월 26일, 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon DataZone의 Preview 릴리스에 대한 전체 액세스를 제공합니다. 또한 관련 서비스에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZonePreviewConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 28일, 15:16 UTC
- 편집된 시간: 2023년 7월 13일, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary는 AWS 관리형 정책으로, Amazon DataZone은 데이터 분석 프로젝트를 배포하는 데 사용하는 IAM 역할을 생성합니다. DataZone은 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneProjectDeploymentPermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 21일, 02:54 UTC
- 편집된 시간: 2023년 4월 4일, 02:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZoneProjectRolePermissionsBoundary

`AmazonDataZoneProjectRolePermissionsBoundary`는 AWS 관리형 정책으로, Amazon DataZone은 프로젝트가 데이터 분석 작업을 수행할 수 있도록 IAM 역할을 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneProjectRolePermissionsBoundary를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 21일, 02:51 UTC
- 편집된 시간: 2023년 3월 21일, 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDataZoneRedshiftGlueProvisioningPolicy

`AmazonDataZoneRedshiftGlueProvisioningPolicy`다음과 같은 AWS 관리형 DataZone 정책입니다. Amazon은 데이터를 카탈로그, 검색, 통제, 공유 및 분석할 수 있는 데이터 관리 서비스입니다.

DataZoneAmazon을 사용하면 계정 및 지원 지역 전반에서 데이터를 공유하고 액세스할 수 있습니다. Amazon은 Amazon Redshift, Amazon Athena, AWS Glue 및 Lake Formation을 포함하되 이에 국한되지 않는 AWS 서비스 전반에서 사용자 경험을 DataZone 단순화합니다. AWS

이 정책 사용

사용자, 그룹 및 역할에 AmazonDataZoneRedshiftGlueProvisioningPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2023년 9월 22일, 20:19 UTC
- 편집 시간: 2024년 3월 12일 16:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
```

```
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
```

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

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonDataZoneRedshiftManageAccessRolePolicy

`AmazonDataZoneRedshiftManageAccessRolePolicy`다음과 같은 AWS관리형 정책입니다. 이 정책은 Amazon에 Amazon Redshift 데이터를 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 카탈로그에 있는 Amazon Redshift 또는 Amazon Redshift 서버리스에 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 아마존에 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDataZoneRedshiftManageAccessRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 9월 22일, 20:15 UTC
- 편집 시간: 2023년 11월 16일 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
```

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

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess`는 AWS 관리형 정책으로, Amazon Detective 서비스에 대한 전체 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDetectiveFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 30일, 17:57 UTC
- 편집된 시간: 2023년 5월 17일, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess`는 AWS 관리형 정책으로, Amazon Detective 서비스에 대한 전체 액세스 권한과 콘솔 UI 종속성에 대한 조사자 액세스를 제공합니다. 이 정책은 조사 목적으로 Detective를 사용할 수 있는 권한을 부여하고 Guardduty에 대한 제한된 쓰기 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDetectiveInvestigatorAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 17일, 15:24 UTC
- 편집 시간: 2023년 11월 27일 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDetectiveMemberAccess

`AmazonDetectiveMemberAccess`는 AWS 관리형 정책으로, Amazon Detective 서비스에 대한 멤버 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDetectiveMemberAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2023년 1월 17일, 15:16 UTC
- 편집된 시간: 2023년 1월 17일, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess는 AWS 관리형 정책으로, Amazon Detective 서비스에 대한 위임된 관리자를 관리할 수 있는 Organizations 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스를 제공합니다. 또한 Detective에 대한 서비스 연결 역할을 생성할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDetectiveOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 2일, 15:20 UTC
- 편집된 시간: 2023년 3월 2일, 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDetectiveServiceLinkedRolePolicy

`AmazonDetectiveServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Amazon Detective가 사용자를 대신하여 서비스 호출을 할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 18일, 19:47 UTC
- 편집된 시간: 2021년 11월 18일, 19:47 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess`는 AWS 관리형 정책으로, DevOps Guru 콘솔에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 12월 17일, 18:43 UTC
- 편집된 시간: 2022년 8월 25일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess는 AWS 관리형 정책으로, Amazon DevOps Guru에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:38 UTC
- 편집된 시간: 2022년 8월 25일, 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess는 AWS 관리형 정책으로, 조직 내에서 Amazon DevOps Guru를 활성화하고 관리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDevOpsGuruOrganizationsAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 15일, 23:50 UTC
- 편집된 시간: 2021년 11월 15일, 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess`는 AWS 관리형 정책으로, Amazon DevOps Guru Console에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDevOpsGuruReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:34 UTC
- 편집된 시간: 2022년 8월 25일, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy는 AWS 관리형 정책으로, Amazon DevOpsGuru가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 1일, 10:24 UTC
- 편집된 시간: 2023년 1월 10일, 14:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole는 AWS 관리형 정책으로, 고객 계정의 cloudwatch 로그에 DMS 복제 로그를 업로드할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDMSCloudWatchLogsRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 7일, 23:44 UTC
- 편집된 시간: 2023년 5월 23일, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDMSRedshiftS3Role

`AmazonDMSRedshiftS3Role`는 AWS 관리형 정책으로, DMS용 Redshift 엔드포인트의 S3 설정을 관리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDMSRedshiftS3Role`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 4월 20일, 17:05 UTC
- 편집된 시간: 2019년 7월 8일, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole는 AWS 관리형 정책으로, AWS 관리형 고객 구성에 대한 VPC 설정을 관리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDMSVPCManagementRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 18일, 16:33 UTC
- 편집된 시간: 2016년 5월 23일, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDB-ElasticServiceRolePolicy

`AmazonDocDB-ElasticServiceRolePolicy`는 AWS 관리형 정책으로, Amazon DocumentDB-Elastic이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 30일, 14:17 UTC
- 편집된 시간: 2022년 11월 30일, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDBConsoleFullAccess

`AmazonDocDBConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 사용하여 Amazon DocumentDB(MongoDB 호환)을 관리할 수 있는 전체 액세스를 제공합니다. 참고로 이 정책은 또한 계정 내의 모든 SNS 주제에 대해 게시할 수 있는 전체 액세스, Amazon EC2 인스턴스 및 VPC 구성을 생성 및 편집할 수 있는 권한, Amazon KMS에서 키를 보고 나열할 수 있는 권한, Amazon RDS 및 Amazon Neptune에 대한 전체 액세스도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDocDBConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:37 UTC
- 편집된 시간: 2022년 11월 30일, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
```

```
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
```

```
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDBElasticFullAccess

`AmazonDocDBElasticFullAccess`는 AWS 관리형 정책으로, Amazon DocumentDB Elastic Clusters에 대한 전체 액세스와 EC2, KMS, SecretsManager, CloudWatch 및 IAM을 포함한 종속성에 필요한 기타 필수 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDocDBElasticFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 5일, 13:51 UTC
- 편집된 시간: 2023년 6월 21일, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDBElasticReadOnlyAccess

`AmazonDocDBElasticReadOnlyAccess`는 AWS 관리형 정책으로, Amazon DocDB-Elastic 및 Amazon CloudWatch 지표에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDocDBElasticReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 8일, 14:37 UTC
- 편집된 시간: 2023년 6월 21일, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDBFullAccess

AmazonDocDBFullAccess는 AWS 관리형 정책으로, Amazon DocumentDB(MongoDB 호환)에 대한 전체 액세스를 제공합니다. 참고로 이 정책은 계정 내 모든 SNS 주제에 대한 게시에 대한 전체 액세스와 Amazon RDS 및 Amazon Neptune에 대한 전체 액세스도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDocDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:21 UTC
- 편집된 시간: 2019년 1월 9일, 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDocDBReadOnlyAccess

`AmazonDocDBReadOnlyAccess`는 AWS 관리형 정책으로, Amazon DocumentDB(MongoDB 호환)에 대한 읽기 전용 액세스를 제공합니다. 참고로 이 정책은 Amazon RDS 및 Amazon Neptune 리소스에 대한 액세스 권한도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonDocDBReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 9일, 20:30 UTC
- 편집된 시간: 2019년 1월 9일, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDRSVPCManagement

AmazonDRSVPCManagement는 AWS 관리형 정책으로, Amazon 관리형 고객 구성에 대한 VPC 설정을 관리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDRSVPCManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 9월 2일, 00:09 UTC
- 편집된 시간: 2015년 9월 2일, 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDynamoDBFullAccess

AmazonDynamoDBFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon DynamoDB에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2021년 1월 29일, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDynamoDBFullAccesswithDataPipeline

AmazonDynamoDBFullAccesswithDataPipeline는 AWS 관리형 정책으로, 이 정책은 사용 중단 중입니다. 지침은 설명서를 참조하세요. https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html AWS Management Console을 통해 AWS Data Pipeline을 사용하여 Export/Import를 포함하여 Amazon DynamoDB에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBFullAccesswithDataPipeline를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 11월 12일, 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonDynamoDBReadOnlyAccess

AmazonDynamoDBReadOnlyAccess는 다음을 통해 Amazon DynamoDB에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 AmazonDynamoDBReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 3월 20일 15:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
```

```
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy는 AWS 관리형 정책으로, CSI 드라이버 서비스 계정이 사용자를 대신하여 EC2와 같은 관련 서비스를 호출할 수 있도록 허용하는 IAM 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEBSCSIDriverPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 4일, 17:24 UTC
- 편집된 시간: 2022년 11월 18일, 14:42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerRegistryFullAccess

`AmazonEC2ContainerRegistryFullAccess`는 AWS 관리형 정책으로, Amazon ECR 리소스에 대한 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ContainerRegistryFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:06 UTC
- 편집된 시간: 2020년 12월 5일, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerRegistryPowerUser

AmazonEC2ContainerRegistryPowerUser는 AWS 관리형 정책으로, Amazon EC2 Container Registry 리포지토리에 대한 전체 액세스를 제공하지만 리포지토리 삭제 또는 정책 변경은 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerRegistryPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:05 UTC
- 편집된 시간: 2019년 12월 10일, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerRegistryReadOnly

`AmazonEC2ContainerRegistryReadOnly`는 AWS 관리형 정책으로, Amazon EC2 Container Registry 리포지토리에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ContainerRegistryReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 21일, 17:04 UTC
- 편집된 시간: 2019년 12월 10일, 20:56 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole는 AWS 관리형 정책으로, Amazon EC2 Container Service에 대해 Task Autoscaling을 활성화하기 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2ContainerServiceAutoscaleRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 5월 12일, 23:25 UTC
- 편집된 시간: 2018년 2월 5일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerServiceEventsRole

`AmazonEC2ContainerServiceEventsRole`는 AWS 관리형 정책으로, EC2 Container Service스에 대해 CloudWatch 이벤트를 활성화하기 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ContainerServiceEventsRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 5월 30일, 16:51 UTC
- 편집된 시간: 2023년 3월 6일, 22:25 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerServiceforEC2Role

`AmazonEC2ContainerServiceforEC2Role`은 AWS 관리형 정책으로, Amazon EC2 Container Service의 Amazon EC2 Role에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ContainerServiceforEC2Role`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 3월 19일, 18:45 UTC
- 편집된 시간: 2023년 3월 6일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ContainerServiceRole

`AmazonEC2ContainerServiceRole`는 AWS 관리형 정책으로, Amazon ECS 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ContainerServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 16:14 UTC
- 편집된 시간: 2016년 8월 11일, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2FullAccess

`AmazonEC2FullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon EC2에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC

- 편집된 시간: 2018년 11월 27일, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2ReadOnlyAccess

`AmazonEC2ReadOnlyAccess`는 다음을 통해 Amazon EC2에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 2월 14일 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy는 AWS 관리형 정책으로, 개정을 다운로드할 수 있도록 S3 버킷에 대한 EC2 액세스를 제공합니다. 이 역할은 EC2 인스턴스의 CodeDeploy 에이전트에 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforAWSCodeDeploy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 19일, 18:10 UTC
- 편집된 시간: 2017년 3월 20일, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2RoleforAWSCodeDeployLimited

`AmazonEC2RoleforAWSCodeDeployLimited`는 AWS 관리형 정책으로, 개정을 다운로드할 수 있도록 S3 버킷에 대한 EC2 제한된 액세스를 제공합니다. 이 역할은 EC2 인스턴스의 CodeDeploy 에이전트에 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2RoleforAWSCodeDeployLimited`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 24일, 17:55 UTC
- 편집된 시간: 2022년 1월 20일, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole는 AWS 관리형 정책으로, Amazon EC2 Role for Data Pipeline 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RoleforDataPipelineRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2016년 2월 22일, 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2RoleforSSM

`AmazonEC2RoleforSSM`는 AWS 관리형 정책으로, 이 정책은 곧 지원 중단될 예정입니다. EC2 인스턴스에서 AmazonSSMManagedInstanceCore 정책을 사용하여 AWS Systems Manager 서비스 핵심 기능을 활성화하세요. 자세한 내용은 https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html을 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2RoleforSSM`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 29일, 17:48 UTC
- 편집된 시간: 2019년 1월 24일, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2RolePolicyForLaunchWizard

`AmazonEC2RolePolicyForLaunchWizard`는 AWS 관리형 정책으로, EC2의 Amazon LaunchWizard 서비스 역할에 대한 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEC2RolePolicyForLaunchWizard를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 08:05 UTC
- 편집된 시간: 2022년 5월 16일, 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2SpotFleetAutoscaleRole

`AmazonEC2SpotFleetAutoscaleRole`는 AWS 관리형 정책으로, Amazon EC2 Spot Fleet에 대해 Autoscaling을 활성화하기 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2SpotFleetAutoscaleRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 8월 19일, 18:27 UTC
- 편집된 시간: 2019년 2월 18일, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEC2SpotFleetTaggingRole

`AmazonEC2SpotFleetTaggingRole`는 AWS 관리형 정책으로, EC2 Spot Fleet이 사용자를 대신하여 Spot Instances를 요청, 종료 및 태그 지정할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEC2SpotFleetTaggingRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 6월 29일, 18:19 UTC
- 편집된 시간: 2020년 4월 23일, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonECS_FullAccess

`AmazonECS_FullAccess`는 AWS 관리형 정책으로, Amazon ECS 리소스에 대한 관리자 액세스를 제공하고 VPC, Auto Scaling 그룹 및 CloudFormation 스택을 포함한 기타 AWS 서비스 리소스에 대한 액세스를 통해 ECS 기능을 활성화합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonECS_FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 7일, 21:36 UTC
- 편집된 시간: 2023년 1월 4일, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

정책 버전

정책 버전: v20(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
```

```
            "codedeploy:BatchGetApplications",
            "codedeploy:BatchGetDeploymentGroups",
            "codedeploy:BatchGetDeployments",
            "codedeploy:ContinueDeployment",
            "codedeploy:CreateApplication",
            "codedeploy:CreateDeployment",
            "codedeploy:CreateDeploymentGroup",
            "codedeploy:GetApplication",
            "codedeploy:GetApplicationRevision",
            "codedeploy:GetDeployment",
            "codedeploy:GetDeploymentConfig",
            "codedeploy:GetDeploymentGroup",
            "codedeploy:GetDeploymentTarget",
            "codedeploy:ListApplicationRevisions",
            "codedeploy:ListApplications",
            "codedeploy:ListDeploymentConfigs",
            "codedeploy:ListDeploymentGroups",
            "codedeploy:ListDeployments",
            "codedeploy:ListDeploymentTargets",
            "codedeploy:RegisterApplicationRevision",
            "codedeploy:StopDeployment",
            "ec2:AssociateRouteTable",
            "ec2:AttachInternetGateway",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CancelSpotFleetRequests",
            "ec2:CreateInternetGateway",
            "ec2:CreateLaunchTemplate",
            "ec2:CreateRoute",
            "ec2:CreateRouteTable",
            "ec2:CreateSecurityGroup",
            "ec2:CreateSubnet",
            "ec2:CreateVpc",
            "ec2:DeleteLaunchTemplate",
            "ec2:DeleteSubnet",
            "ec2:DeleteVpc",
            "ec2:Describe*",
            "ec2:DetachInternetGateway",
            "ec2:DisassociateRouteTable",
            "ec2:ModifySubnetAttribute",
            "ec2:ModifyVpcAttribute",
            "ec2:RequestSpotFleet",
            "ec2:RunInstances",
            "ecs:*",
            "elasticfilesystem:DescribeAccessPoints",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`는 사용자를 대신하여 ECS Service Connect TLS 기능을 관리하는 AWS 서비스 데 필요한 사설 인증 기관, AWS Secrets Manager 및 기타 시스템에 대한 관리 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2024년 1월 19일 20:08 UTC
- 편집 시간: 2024년 1월 19일 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonECSInfrastructureRolePolicyForVolumes

`AmazonECSInfrastructureRolePolicyForVolumes`사용자를 대신하여 ECS 워크로드와 관련된 볼륨을 관리하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonECSInfrastructureRolePolicyForVolumes를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2024년 1월 10일 22:56 UTC
- 편집 시간: 2024년 1월 10일 22:56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy는 AWS 관리형 정책으로, Amazon ECS가 클러스터를 관리할 수 있도록 지원하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2017년 10월 14일, 01:18 UTC
- 편집 시간: 2023년 12월 4일 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy는 AWS 관리형 정책으로, Amazon ECS 태스크를 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonECSTaskExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 16일, 18:48 UTC
- 편집된 시간: 2017년 11월 16일, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy는 AWS 관리형 정책으로, EFS 리소스에 대한 관리 액세스와 EC2에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEFSCSIDriverPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 7월 25일, 20:10 UTC
- 편집된 시간: 2023년 7월 25일, 20:10 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKS_CNI_Policy

AmazonEKS_CNI_Policy는 다음과 같은 AWS 관리형 정책입니다. 이 정책은 Amazon VPC CNI 플러그인 (amazon-vpc-cni-k8s) 에 EKS 작업자 노드의 IP 주소 구성을 수정하는 데 필요한 권한을 제공합니다. 이 권한 세트를 통해 CNI는 사용자를 대신하여 Elastic Network Interfaces를 나열, 설명 및 수정할 수 있습니다. AWS VPC CNI 플러그인에 대한 자세한 내용은 다음에서 확인할 수 있습니다. https://github.com/aws/ 8s amazon-vpc-cni-k

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKS_CNI_Policy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2018년 5월 27일, 21:07 UTC
- 편집 시간: 2024년 3월 4일 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonEKSClusterPolicy

`AmazonEKSClusterPolicy`는 AWS 관리형 정책으로, 이 정책은 Kubernetes가 사용자를 대신하여 리소스를 관리하는 데 필요한 권한을 제공합니다. Kubernetes에서는 Instances, Security Groups, Elastic Network Interfaces를 포함하되 이에 국한되지 않는 EC2 리소스에 식별 정보를 배치하려면 EC2:CreateTags 권한이 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSClusterPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:06 UTC
- 편집된 시간: 2023년 2월 7일, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
```

```
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSConnectorServiceRolePolicy

`AmazonEKSConnectorServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 Amazon EKS가 EKS 커넥터의 AWS 리소스를 관리할 수 있도록 허용하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2021년 9월 4일, 20:31 UTC
- 편집된 시간: 2021년 9월 4일, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy는 AWS 관리형 정책으로, AWS Fargate에서 Amazon EKS 포드를 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSFargatePodExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 22일, 04:34 UTC
- 편집된 시간: 2019년 11월 22일, 04:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSForFargateServiceRolePolicy

`AmazonEKSForFargateServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 Fargate 태스크를 실행하는 데 필요한 권한을 Amazon EKS에 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 22일, 04:36 UTC
- 편집된 시간: 2019년 11월 22일, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy는 AWS 관리형 정책으로, 이 정책은 사용자를 대신하여 리소스를 관리하기 위해 계정에서 실행 중인 EKS 로컬 클러스터의 컨트롤 플레인 인스턴스에 대한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSLocalOutpostClusterPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 24일, 21:56 UTC
- 편집된 시간: 2022년 10월 17일, 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
```

```
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSLocalOutpostServiceRolePolicy

`AmazonEKSLocalOutpostServiceRolePolicy`는 AWS 관리형 정책으로, Amazon EKS Local이 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 8월 23일, 21:53 UTC

- 편집된 시간: 2022년 10월 24일, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSServicePolicy

AmazonEKSServicePolicy는 AWS 관리형 정책으로, 이 정책은 Amazon Elastic Container Service for Kubernetes가 EKS Clusters를 운영하는 데 필요한 리소스를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSServicePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:08 UTC
- 편집된 시간: 2020년 5월 27일, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSServiceRolePolicy

`AmazonEKSServiceRolePolicy`는 AWS 관리형 정책으로, Amazon EKS가 사용자를 대신하여 AWS 서비스를 호출하는 데 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 2월 21일, 20:10 UTC
- 편집된 시간: 2020년 5월 27일, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterfacePermission",
        "iam:ListAttachedRolePolicies",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ],
          "aws:RequestTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSVPCResourceController

`AmazonEKSVPCResourceController`는 AWS 관리형 정책으로, VPC Resource Controller가 워커 노드의 ENI와 IP를 관리하기 위해 사용하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEKSVPCResourceController`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 12일, 00:55 UTC
- 편집된 시간: 2020년 8월 12일, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy는 AWS 관리형 정책으로, 이 정책은 Amazon EKS 워커 노드가 Amazon EKS Clusters에 연결할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEKSWorkerNodePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 27일, 21:09 UTC
- 편집 시간: 2023년 11월 27일 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElastiCacheFullAccess

`AmazonElastiCacheFullAccess`는 다음을 ElastiCache 통해 Amazon에 대한 전체 액세스를 제공하는 AWS관리형 AWS Management Console 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElastiCacheFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 11월 28일 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElastiCacheReadOnlyAccess

`AmazonElastiCacheReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon ElastiCache에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElastiCacheReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticContainerRegistryPublicFullAccess

`AmazonElasticContainerRegistryPublicFullAccess`는 AWS 관리형 정책으로, Amazon ECR Public 리소스에 대한 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticContainerRegistryPublicFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 17:25 UTC
- 편집된 시간: 2020년 12월 1일, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser는 AWS 관리형 정책으로, Amazon ECR Public 리포지토리에 대한 전체 액세스를 제공하지만 리포지토리 삭제 또는 정책 변경은 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticContainerRegistryPublicPowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:16 UTC
- 편집된 시간: 2020년 12월 1일, 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticContainerRegistryPublicReadOnly

`AmazonElasticContainerRegistryPublicReadOnly`는 AWS 관리형 정책으로, Amazon ECR Public 리포지토리에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticContainerRegistryPublicReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 17:27 UTC

- 편집된 시간: 2020년 12월 1일, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess는 AWS 관리형 정책으로, Amazon EFS 파일 시스템에 대한 루트 클라이언트 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemClientFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 13일, 16:27 UTC
- 편집된 시간: 2020년 1월 13일, 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemClientReadOnlyAccess

`AmazonElasticFileSystemClientReadOnlyAccess`는 AWS 관리형 정책으로, Amazon EFS 파일 시스템에 대한 읽기 전용 클라이언트 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticFileSystemClientReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 13일, 16:24 UTC
- 편집된 시간: 2020년 1월 13일, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemClientReadWriteAccess

`AmazonElasticFileSystemClientReadWriteAccess`는 AWS 관리형 정책으로, Amazon EFS 파일 시스템에 대한 읽기 및 쓰기 클라이언트 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticFileSystemClientReadWriteAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 13일, 16:21 UTC
- 편집된 시간: 2020년 1월 13일, 16:21 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemFullAccess

`AmazonElasticFileSystemFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon EFS에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 27일, 16:22 UTC
- 편집 시간: 2023년 11월 28일 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
```

```
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemReadOnlyAccess

`AmazonElasticFileSystemReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon EFS에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticFileSystemReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 27일, 16:25 UTC
- 편집된 시간: 2022년 1월 10일, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemServiceRolePolicy

AmazonElasticFileSystemServiceRolePolicy는 AWS 관리형 정책으로, Amazon Elastic File System이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 5일, 16:52 UTC
- 편집된 시간: 2022년 1월 10일, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticFileSystemsUtils

AmazonElasticFileSystemsUtils는 AWS 관리형 정책으로, 고객이 AWS Systems Manager를 사용하여 EC2 인스턴스에서 Amazon EFS 유틸리티(amazon-efs-utils) 패키지를 자동으로 관리하고 CloudWatchLog를 사용하여 EFS 파일 시스템 탑재 성공/실패 알림을 받을 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticFileSystemsUtils를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 29일, 15:16 UTC
- 편집된 시간: 2020년 9월 29일, 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceEditorsRole

`AmazonElasticMapReduceEditorsRole`는 AWS 관리형 정책으로, Amazon Elastic MapReduce Editors 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticMapReduceEditorsRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 16일, 21:55 UTC
- 편집된 시간: 2023년 2월 9일, 22:39 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceforAutoScalingRole

`AmazonElasticMapReduceforAutoScalingRole`는 AWS 관리형 정책으로, Auto Scaling을 위한 Amazon Elastic MapReduce입니다. Auto Scaling이 EMR 클러스터에서 인스턴스를 추가 및 제거할 수 있도록 허용하는 역할입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticMapReduceforAutoScalingRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 18일, 01:09 UTC
- 편집된 시간: 2016년 11월 18일, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceforEC2Role

`AmazonElasticMapReduceforEC2Role`는 AWS 관리형 정책으로, Amazon Elastic MapReduce for EC2 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceforEC2Role를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2017년 8월 11일, 23:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceFullAccess

AmazonElasticMapReduceFullAccess는 AWS 관리형 정책으로, 이 정책은 사용 중단 중입니다. 지침은 설명서를 참조하세요. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html Amazon Elastic MapReduce와 이에 필요한 기본 서비 (예: EC2, S3)에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 10월 11일, 15:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReducePlacementGroupPolicy

`AmazonElasticMapReducePlacementGroupPolicy`는 AWS 관리형 정책으로, EMR이 EC2 배치 그룹을 생성, 설명 및 삭제할 수 있도록 허용하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticMapReducePlacementGroupPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 29일, 00:37 UTC
- 편집된 시간: 2020년 9월 29일, 00:37 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceReadOnlyAccess

AmazonElasticMapReduceReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Elastic MapReduce에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticMapReduceReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 7월 29일, 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticMapReduceRole

`AmazonElasticMapReduceRole`는 AWS 관리형 정책으로, 이 정책은 사용 중단 중입니다. 지침은 설명서를 참조하세요. https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html Amazon Elastic MapReduce 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticMapReduceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2020년 6월 24일, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticsearchServiceRolePolicy

`AmazonElasticsearchServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Elasticsearch Service가 사용자를 대신하여 EC2 네트워킹 API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 7월 7일, 00:15 UTC
- 편집된 시간: 2023년 10월 23일, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticTranscoder_FullAccess

AmazonElasticTranscoder_FullAccess는 AWS 관리형 정책으로, 사용자에게 Elastic Transcoder에 대한 전체 액세스 권한과 전체 Elastic Transcoder 기능에 필요한 연관된 서비스에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoder_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 27일, 18:59 UTC
- 편집된 시간: 2019년 6월 10일, 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticTranscoder_JobsSubmitter

`AmazonElasticTranscoder_JobsSubmitter`는 AWS 관리형 정책으로, 사용자에게 사전 설정을 변경하고, 작업을 제출하고, Elastic Transcoder 설정을 볼 수 있는 권한을 부여합니다. 또한 이 정책은 Elastic Transcode 콘솔을 사용하는 데 필요한 일부 다른 서비스(S3, IAM, SNS등)에 대한 읽기 전용 액세스 권한도 일부 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticTranscoder_JobsSubmitter`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 7일, 21:12 UTC
- 편집된 시간: 2019년 6월 10일, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticTranscoder_ReadOnlyAccess

AmazonElasticTranscoder_ReadOnlyAccess는 AWS 관리형 정책으로, 사용자에게 Elastic Transcoder에 대한 읽기 전용 액세스 권한과 관련 서비스에 대한 목록 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonElasticTranscoder_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 7일, 21:09 UTC
- 편집된 시간: 2019년 6월 10일, 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonElasticTranscoderRole

`AmazonElasticTranscoderRole`는 AWS 관리형 정책으로, Amazon Elastic Transcoder 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonElasticTranscoderRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2019년 6월 13일, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRCleanupPolicy

AmazonEMRCleanupPolicy는 AWS 관리형 정책으로, EMR Service 역할이 해당 기능을 상실한 경우 EMR이 AWS EC2 리소스를 종료 및 삭제하는 데 필요한 작업을 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 26일, 23:54 UTC
- 편집된 시간: 2020년 9월 29일, 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRContainersServiceRolePolicy

`AmazonEMRContainersServiceRolePolicy`는 AWS 관리형 정책으로, Amazon EMR을 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 9일, 00:38 UTC
- 편집된 시간: 2023년 3월 10일, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRFullAccessPolicy_v2

AmazonEMRFullAccessPolicy_v2는 AWS 관리형 정책으로, Amazon EMR에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRFullAccessPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 12일, 01:50 UTC
- 편집된 시간: 2023년 7월 28일, 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
```

```
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRReadOnlyAccessPolicy_v2

AmazonEMRReadOnlyAccessPolicy_v2는 AWS 관리형 정책으로, Amazon EMR 및 연관된 CloudWatch Metrics에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRReadOnlyAccessPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 12일, 01:39 UTC

- 편집된 시간: 2023년 8월 2일, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRServerlessServiceRolePolicy

`AmazonEMRServerlessServiceRolePolicy`는 AWS 관리형 정책으로, Amazon EMRServerless를 실행하는 데 필요한 다른 AWS 서비스 리소스에 대한 액세스를 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 5월 20일, 23:15 UTC
- 편집 시간: 2024년 1월 25일 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEMRServicePolicy_v2

AmazonEMRServicePolicy_v2는 AWS 관리형 정책으로, 이 정책은 Amazon EMR 서비스 역할에 사용되며 계정의 다른 IAM 사용자 또는 역할에는 사용해서는 안 됩니다. 이 정책은 EMR 클러스터 운영에 필요한 EMR 및 관련 서비스와 연관된 리소스를 생성하고 관리할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEMRServicePolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 3월 12일, 01:11 UTC
- 편집된 시간: 2022년 2월 15일, 16:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
```

```
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonESCognitoAccess

AmazonESCognitoAccess는 AWS 관리형 정책으로, Amazon Cognito 구성 서비스에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonESCognitoAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 28일, 22:29 UTC
- 편집된 시간: 2021년 12월 20일, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonESFullAccess

AmazonESFullAccess는 AWS 관리형 정책으로, Amazon ES 구성 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonESFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 1일, 19:14 UTC
- 편집된 시간: 2015년 10월 1일, 19:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonESReadOnlyAccess

`AmazonESReadOnlyAccess`는 AWS 관리형 정책으로, Amazon ES 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonESReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 1일, 19:18 UTC
- 편집된 시간: 2018년 10월 3일, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicy는 AWS 관리형 정책으로, EventBridge가 사용자를 대신하여 Secret Manager 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 2월 11일, 20:52 UTC
- 편집된 시간: 2021년 2월 11일, 20:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeFullAccess

`AmazonEventBridgeFullAccess`는 AWS 관리형 정책으로, Amazon EventBridge에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEventBridgeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 11일, 14:08 UTC
- 편집된 시간: 2022년 12월 1일, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgePipesFullAccess

`AmazonEventBridgePipesFullAccess`는 AWS 관리형 정책으로, Amazon EventBridge Pipes에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEventBridgePipesFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 12월 1일, 17:03 UTC
- 편집된 시간: 2022년 12월 1일, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess는 AWS 관리형 정책으로, Amazon EventBridge Pipes에 대한 읽기 전용 및 운영자(파이프 실행 중지 및 시작 기능) 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgePipesOperatorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 12월 1일, 17:04 UTC
- 편집된 시간: 2022년 12월 1일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgePipesReadOnlyAccess

AmazonEventBridgePipesReadOnlyAccess는 AWS 관리형 정책으로, Amazon EventBridge Pipes에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgePipesReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 12월 1일, 17:04 UTC
- 편집된 시간: 2022년 12월 1일, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeReadOnlyAccess

`AmazonEventBridgeReadOnlyAccess`는 AWS 관리형 정책으로, Amazon EventBridge에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEventBridgeReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 11일, 13:59 UTC
- 편집된 시간: 2022년 12월 1일, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeSchedulerFullAccess

`AmazonEventBridgeSchedulerFullAccess`는 AWS 관리형 정책으로, 일정과 일정 그룹에 대한 모든 EventBridge Scheduler 작업을 사용할 수 있는 권한을 부여하는 AmazonEventBridgeSchedulerFullAccess 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEventBridgeSchedulerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 18:37 UTC
- 편집된 시간: 2022년 11월 10일, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeSchedulerReadOnlyAccess

`AmazonEventBridgeSchedulerReadOnlyAccess`는 AWS 관리형 정책으로, 일정 및 일정 그룹에 대한 세부 정보를 볼 수 있는 읽기 전용 권한을 부여하는 Amazon AmazonEventBridgeSchedulerReadOnlyAccess 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchedulerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 18:50 UTC
- 편집된 시간: 2022년 11월 10일, 18:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeSchemasFullAccess

`AmazonEventBridgeSchemasFullAccess`는 AWS 관리형 정책으로, Amazon EventBridge에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonEventBridgeSchemasFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 28일, 23:12 UTC
- 편집된 시간: 2019년 11월 28일, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess는 AWS 관리형 정책으로, Amazon EventBridge Schemas에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonEventBridgeSchemasReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 28일, 23:05 UTC
- 편집된 시간: 2020년 5월 1일, 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonEventBridgeSchemasServiceRolePolicy

`AmazonEventBridgeSchemasServiceRolePolicy`는 AWS 관리형 정책으로, Amazon EventBridge 스키마에서 생성된 관리형 규칙에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 27일, 01:10 UTC
- 편집된 시간: 2019년 11월 27일, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy는 AWS 관리형 정책으로, AWS FIS가 실험을 위한 모니터링 및 리소스 선택을 관리할 수 있도록 활성화하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 21일, 21:18 UTC
- 편집된 시간: 2022년 10월 25일, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonForecastFullAccess

AmazonForecastFullAccess는 AWS 관리형 정책으로, Amazon Forecast의 모든 작업에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonForecastFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 01:52 UTC
- 편집된 시간: 2019년 1월 18일, 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFraudDetectorFullAccessPolicy

`AmazonFraudDetectorFullAccessPolicy`는 AWS 관리형 정책으로, Amazon Fraud Detector의 모든 작업에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonFraudDetectorFullAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 22:46 UTC
- 편집된 시간: 2019년 12월 3일, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFreeRTOSFullAccess

`AmazonFreeRTOSFullAccess`는 AWS 관리형 정책으로, Amazon FreeRTOS에 대한 전체 액세스 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonFreeRTOSFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 15:32 UTC
- 편집된 시간: 2017년 11월 29일, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFreeRTOSOTAUpdate

AmazonFreeRTOSOTAUpdate는 AWS 관리형 정책으로, 사용자가 Amazon FreeRTOS OTA 업데이트에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFreeRTOSOTAUpdate를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 8월 27일, 22:43 UTC
- 편집된 시간: 2020년 12월 18일, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFSxConsoleFullAccess

`AmazonFSxConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon FSx에 대한 전체 액세스와 관련 AWS 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonFSxConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:36 UTC
- 편집 시간: 2024년 1월 10일 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
```

```
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFSxConsoleReadOnlyAccess

`AmazonFSxConsoleReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon FSx에 대한 읽기 전용 액세스와 관련 AWS 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonFSxConsoleReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:35 UTC
- 편집 시간: 2024년 1월 10일 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFSxFullAccess

AmazonFSxFullAccess는 AWS 관리형 정책으로, Amazon FSx에 대한 전체 액세스와 관련 AWS 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:34 UTC
- 편집 시간: 2024년 1월 10일 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
```

```
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
```

```
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
```

```
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFSxReadOnlyAccess

`AmazonFSxReadOnlyAccess`는 AWS 관리형 정책으로, Amazon FSx에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonFSxReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 16:33 UTC
- 편집된 시간: 2018년 11월 28일, 16:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonFSxServiceRolePolicy

AmazonFSxServiceRolePolicy는 AWS 관리형 정책으로, Amazon FSx이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 28일, 10:38 UTC
- 편집 시간: 2024년 1월 10일 20:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGlacierFullAccess

`AmazonGlacierFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Glacier에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonGlacierFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGlacierReadOnlyAccess

`AmazonGlacierReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Glacier에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonGlacierReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 5월 5일, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGrafanaAthenaAccess

`AmazonGrafanaAthenaAccess`는 AWS 관리형 정책으로, 이 정책은 Amazon Athena 및 Amazon Grafana의 Amazon Athena 플러그인에서 s3에 결과를 쿼리하고 작성하는 데 필요한 종속성에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonGrafanaAthenaAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 22일, 17:11 UTC
- 편집된 시간: 2021년 11월 22일, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGrafanaCloudWatchAccess

`AmazonGrafanaCloudWatchAccess`는 AWS 관리형 정책으로, 이 정책은 Amazon CloudWatch 및 Amazon Managed Grafana 내에서 CloudWatch를 데이터 소스로 사용하는 데 필요한 종속성에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonGrafanaCloudWatchAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 3월 24일, 22:41 UTC
- 편집된 시간: 2023년 3월 24일, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGrafanaRedshiftAccess

AmazonGrafanaRedshiftAccess는 AWS 관리형 정책으로, 이 정책은 Amazon Redshift 및 Amazon Grafana의 Amazon Redshift 플러그인을 사용하는 데 필요한 종속성에 대한 범위 지정된 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGrafanaRedshiftAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 26일, 23:15 UTC
- 편집된 시간: 2021년 11월 26일, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy는 AWS 관리형 정책으로, Amazon Grafana에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 8일, 23:10 UTC
- 편집된 시간: 2022년 11월 8일, 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccessAmazon을 사용하기 위한 전체 액세스 권한을 제공하는 AWS관리형 GuardDuty 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGuardDutyFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 28일, 22:31 UTC
- 편집 시간: 2023년 11월 16일 23:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGuardDutyMalwareProtectionServiceRolePolicy

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` GuardDuty 멀웨어 보호는 이름이 지정된 서비스 연결 역할 (SLR) 을 사용하는 AWS관리형 정책입니다. AWSServiceRoleForAmazonGuardDutyMalwareProtection 이 서비스 연결 역할을 통해 GuardDuty 맬웨어 보호 기능은 에이전트 없이 검사를 수행하여 맬웨어를 탐지할 수 있습니다. GuardDuty 이를 통해 계정에서 스냅샷을 만들고 이 스냅샷을 서비스 계정과 공유하여 멀웨어를 검사할 수 있습니다. GuardDuty 이러한 공유 스냅샷을 평가하여 검색된 EC2 인스턴스 메타데이터를 멀웨어 보호 결과에 포함합니다. GuardDuty AWSServiceRoleForAmazonGuardDutyMalwareProtection 서비스 연결 역할은 멀웨어 보호.guardduty.amazonaws.com 서비스가 역할을 맡을 것으로 신뢰합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 19일, 19:06 UTC
- 편집 시간: 2024년 1월 25일 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccessAmazon GuardDuty 리소스에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonGuardDutyReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 28일, 22:29 UTC
- 편집 시간: 2023년 11월 16일 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonGuardDutyServiceRolePolicy

`AmazonGuardDutyServiceRolePolicy`Amazon Guard AWS Duty에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화하는 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 28일, 20:12 UTC
- 편집 시간: 2024년 2월 9일 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
```

```
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
```

```
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonHealthLakeFullAccess

`AmazonHealthLakeFullAccess`는 AWS 관리형 정책으로, Amazon HealthLake 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonHealthLakeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 01:07 UTC
- 편집된 시간: 2021년 2월 17일, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess는 AWS 관리형 정책으로, Amazon HealthLake 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHealthLakeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 02:43 UTC
- 편집된 시간: 2021년 2월 17일, 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeFullAccess

`AmazonHoneycodeFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonHoneycodeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 6월 24일, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy는 AWS 관리형 정책으로, Amazon Honeycode가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 18일, 18:03 UTC
- 편집된 시간: 2020년 11월 18일, 18:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode Team Association에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeTeamAssociationFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 6월 24일, 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeTeamAssociationReadOnlyAccess

AmazonHoneycodeTeamAssociationReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode Team Association에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonHoneycodeTeamAssociationReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:27 UTC
- 편집된 시간: 2020년 6월 24일, 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeWorkbookFullAccess

`AmazonHoneycodeWorkbookFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode Workbook에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonHoneycodeWorkbookFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonHoneycodeWorkbookReadOnlyAccess

`AmazonHoneycodeWorkbookReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Honeycode Workbook에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonHoneycodeWorkbookReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 20:28 UTC
- 편집된 시간: 2020년 12월 1일, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspector2AgentlessServiceRolePolicy

`AmazonInspector2AgentlessServiceRolePolicy`는 다음과 같은 AWS관리형 정책입니다. Amazon Inspector에 에이전트 없는 보안 평가를 수행하는 데 AWS 서비스 필요한 액세스 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 20일, 15:18 UTC
- 편집 시간: 2023년 11월 20일, 15:18 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspector2FullAccess

AmazonInspector2FullAccess는 AWS 관리형 정책으로, Amazon Inspector에 대한 전체 액세스 권한과 조직 등 기타 관련 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspector2FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 19:10 UTC
- 편집된 시간: 2023년 8월 3일, 19:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "inspector2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspector2ManagedCisPolicy

`AmazonInspector2ManagedCisPolicy`다음과 같은 AWS관리형 정책입니다. 이 정책은 고객이 자신의 역할에 연결하여 CIS 스캔을 위해 검사관 서비스와 통신해야 하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspector2ManagedCisPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 1월 24일 16:31 UTC
- 편집 시간: 2024년 1월 24일 16:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspector2ReadOnlyAccess

`AmazonInspector2ReadOnlyAccess`는 AWS 관리형 정책으로, Amazon inspector2 서비스 및 관련 지원 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonInspector2ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 1월 21일, 14:45 UTC
- 편집된 시간: 2023년 9월 22일, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspector2ServiceRolePolicy

`AmazonInspector2ServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Inspector에 보안 평가를 수행하는 데 필요한 AWS 서비스 서비스에 대한 액세스를 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2021년 11월 16일, 20:27 UTC
- 편집 시간: 2024년 1월 22일 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
```

```
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
```

```
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspectorFullAccess

`AmazonInspectorFullAccess`는 AWS 관리형 정책으로, Amazon Inspector에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonInspectorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 17:08 UTC
- 편집된 시간: 2017년 12월 21일, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspectorReadOnlyAccess

`AmazonInspectorReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Inspector에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonInspectorReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 17:08 UTC
- 편집된 시간: 2019년 10월 1일, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonInspectorServiceRolePolicy

`AmazonInspectorServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Inspector에 보안 평가를 수행하는 데 필요한 AWS 서비스 서비스에 대한 액세스를 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 21일, 15:48 UTC
- 편집된 시간: 2020년 9월 11일, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKendraFullAccess

`AmazonKendraFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Kendra에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKendraFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:15 UTC
- 편집된 시간: 2019년 12월 3일, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKendraReadOnlyAccess

AmazonKendraReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Kendra에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKendraReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:13 UTC
- 편집된 시간: 2021년 5월 27일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKeyspacesFullAccess

`AmazonKeyspacesFullAccess`는 AWS 관리형 정책으로, Amazon Keyspaces에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKeyspacesFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 23일, 17:06 UTC
- 편집된 시간: 2023년 10월 3일, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKeyspacesReadOnlyAccess

AmazonKeyspacesReadOnlyAccess는 AWS 관리형 정책으로, Amazon Keyspaces에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKeyspacesReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 23일, 17:07 UTC
- 편집된 시간: 2022년 7월 7일, 14:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKeyspacesReadOnlyAccess_v2

`AmazonKeyspacesReadOnlyAccess_v2`는 AWS 관리형 정책으로, Amazon Keyspaces 및 관련 AWS 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKeyspacesReadOnlyAccess_v2`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 12일, 17:01 UTC
- 편집된 시간: 2023년 9월 12일, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisAnalyticsFullAccess

`AmazonKinesisAnalyticsFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Kinesis Analytics에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisAnalyticsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 9월 21일, 19:01 UTC
- 편집된 시간: 2016년 9월 21일, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisAnalyticsReadOnly

`AmazonKinesisAnalyticsReadOnly`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Kinesis Analytics에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisAnalyticsReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 9월 21일, 18:16 UTC
- 편집된 시간: 2016년 9월 21일, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisFirehoseFullAccess

`AmazonKinesisFirehoseFullAccess`는 AWS 관리형 정책으로, 모든 Amazon Kinesis Firehose 전송 스트림에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisFirehoseFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 18:45 UTC
- 편집된 시간: 2015년 10월 7일, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisFirehoseReadOnlyAccess

`AmazonKinesisFirehoseReadOnlyAccess`는 AWS 관리형 정책으로, 모든 Amazon Kinesis Firehose 전송 스트림에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisFirehoseReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 7일, 18:43 UTC
- 편집된 시간: 2015년 10월 7일, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisFullAccess

AmazonKinesisFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 스트림에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonKinesisFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisReadOnlyAccess

`AmazonKinesisReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 스트림에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisVideoStreamsFullAccess

`AmazonKinesisVideoStreamsFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Kinesis Video Streams에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisVideoStreamsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 1일, 23:27 UTC
- 편집된 시간: 2017년 12월 1일, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonKinesisVideoStreamsReadOnlyAccess

`AmazonKinesisVideoStreamsReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Kinesis Video Streams에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonKinesisVideoStreamsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 1일, 23:14 UTC
- 편집된 시간: 2017년 12월 1일, 23:14 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLaunchWizard_Fullaccess

`AmazonLaunchWizard_Fullaccess`는 AWS 관리형 정책으로, AWS 시작 마법사 및 기타 필수 서비스에 대한 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLaunchWizard_Fullaccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 6일, 17:47 UTC
- 편집된 시간: 2023년 2월 22일, 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLaunchWizardFullAccessV2

`AmazonLaunchWizardFullAccessV2`는 AWS 관리형 정책으로, AWS 시작 마법사 및 기타 필수 서비스에 대한 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLaunchWizardFullAccessV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 1일, 17:14 UTC
- 편집된 시간: 2023년 9월 1일, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLexChannelsAccess

`AmazonLexChannelsAccess`는 AWS 관리형 정책으로, 이 정책은 고객이 채널에서 Lex 런타임을 호출할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 13일, 20:12 UTC
- 편집된 시간: 2021년 1월 13일, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLexFullAccess

`AmazonLexFullAccess`는 다음을 통해 Amazon Lex에 대한 전체 액세스 권한을 제공하는 AWS 관리형 AWS Management Console 정책입니다. 또한 Lex 서비스 연결 역할을 생성하고 Lex에 제한된 Lambda 함수 세트를 호출할 수 있는 권한을 부여할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLexFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:20 UTC
- 편집 시간: 2024년 2월 7일 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
```

```
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonLexReadOnly

AmazonLexReadOnly는 AWS 관리형 정책으로, Amazon Lex에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLexReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:13 UTC
- 편집된 시간: 2023년 1월 31일, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
```

```
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLexReplicationPolicy

AmazonLexReplicationPolicy는 다음과 같은 AWS 관리형 정책입니다. Amazon Lex가 사용자를 대신하여 여러 지역에 Lex 리소스를 복제할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2024년 1월 31일 23:29 UTC
- 편집 시간: 2024년 3월 8일 17:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
```

```
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonLexRunBotsOnly

AmazonLexRunBotsOnly는 AWS 관리형 정책으로, Amazon Lex 대화형 API에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLexRunBotsOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 11일, 23:06 UTC
- 편집된 시간: 2021년 8월 18일, 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLexV2BotPolicy

AmazonLexV2BotPolicy는 AWS 관리형 정책으로, Lex V2 봇이 사용자를 대신하여 다른 AWS 서비스를 호출할 수 있는 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 13일, 20:10 UTC
- 편집된 시간: 2021년 1월 13일, 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutEquipmentFullAccess

`AmazonLookoutEquipmentFullAccess`는 AWS 관리형 정책으로, Amazon Lookout for Equipment 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutEquipmentFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 8일, 15:52 UTC
- 편집된 시간: 2021년 11월 24일, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutEquipmentReadOnlyAccess

`AmazonLookoutEquipmentReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Lookout for Equipment에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutEquipmentReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 5일, 16:47 UTC
- 편집된 시간: 2022년 11월 10일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutMetricsFullAccess

`AmazonLookoutMetricsFullAccess`는 AWS 관리형 정책으로, Amazon Lookout for Metrics의 모든 작업에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutMetricsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 7일, 00:43 UTC
- 편집된 시간: 2021년 5월 7일, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutMetricsReadOnlyAccess

`AmazonLookoutMetricsReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Lookout for Metrics의 모든 작업에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutMetricsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 7일, 00:43 UTC
- 편집된 시간: 2022년 1월 4일, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutVisionConsoleFullAccess

`AmazonLookoutVisionConsoleFullAccess`는 AWS 관리형 정책으로, Amazon Lookout for Vision에 대한 전체 액세스 권한과 필수 서비스 및 콘솔 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutVisionConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:37 UTC
- 편집된 시간: 2021년 5월 11일, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutVisionConsoleReadOnlyAccess

`AmazonLookoutVisionConsoleReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Lookout for Vision에 대한 읽기 전용 액세스 권한과 필수 서비스 및 콘솔 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:32 UTC
- 편집된 시간: 2021년 12월 9일, 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess는 AWS 관리형 정책으로, Amazon Lookout for Vision에 대한 전체 액세스 권한과 필수 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonLookoutVisionFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:24 UTC
- 편집된 시간: 2021년 5월 11일, 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonLookoutVisionReadOnlyAccess

`AmazonLookoutVisionReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Lookout for Vision에 대한 읽기 전용 액세스 권한과 필수 종속성에 대한 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonLookoutVisionReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 11일, 19:11 UTC
- 편집된 시간: 2021년 12월 9일, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningBatchPredictionsAccess

`AmazonMachineLearningBatchPredictionsAccess`는 AWS 관리형 정책으로, 사용자에게 Amazon Machine Learning 배치 예측을 요청할 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMachineLearningBatchPredictionsAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:12 UTC

- 편집된 시간: 2015년 4월 9일, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningCreateOnlyAccess

AmazonMachineLearningCreateOnlyAccess는 AWS 관리형 정책으로, 예측이 불가능한 Amazon Machine Learning 리소스에 대한 생성 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningCreateOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:18 UTC
- 편집된 시간: 2016년 6월 29일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningFullAccess

`AmazonMachineLearningFullAccess`는 AWS 관리형 정책으로, Amazon Machine Learning 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMachineLearningFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:25 UTC
- 편집된 시간: 2015년 4월 9일, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`는 AWS 관리형 정책으로, Amazon Machine Learning 모델의 실시간 엔드포인트를 생성 및 삭제할 수 있는 권한을 사용자에게 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMachineLearningManageRealTimeEndpointOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:32 UTC
- 편집된 시간: 2015년 4월 9일, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningReadOnlyAccess

`AmazonMachineLearningReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Machine Learning 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMachineLearningReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:40 UTC
- 편집된 시간: 2015년 4월 9일, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningRealTimePredictionOnlyAccess

AmazonMachineLearningRealTimePredictionOnlyAccess는 AWS 관리형 정책으로, 사용자에게 Amazon Machine Learning 실시간 예측을 요청할 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMachineLearningRealTimePredictionOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 17:44 UTC
- 편집된 시간: 2015년 4월 9일, 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMachineLearningRoleforRedshiftDataSourceV3

`AmazonMachineLearningRoleforRedshiftDataSourceV3`는 AWS 관리형 정책으로, Machine Learning이 Redshift Data Source의 Redshift Clusters 및 S3 Staging Locations를 구성하고 사용할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMachineLearningRoleforRedshiftDataSourceV3`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 24일, 18:00 UTC
- 편집된 시간: 2020년 6월 24일, 18:00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMacieFullAccess

AmazonMacieFullAccess는 AWS 관리형 정책으로, Amazon Macie에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 14:54 UTC
- 편집된 시간: 2022년 7월 1일, 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMacieHandshakeRole

`AmazonMacieHandshakeRole`는 AWS 관리형 정책으로, Amazon Macie의 서비스 연결 역할을 생성할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMacieHandshakeRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2018년 6월 28일, 15:46 UTC
- 편집된 시간: 2018년 6월 28일, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMacieReadOnlyAccess

AmazonMacieReadOnlyAccess는 AWS 관리형 정책으로, Amazon Macie에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 15일, 21:50 UTC
- 편집된 시간: 2023년 6월 15일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMacieServiceRole

AmazonMacieServiceRole는 AWS 관리형 정책으로, 데이터 분석을 활성화하기 위해 Macie에 계정의 리소스 종속성에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMacieServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 14:53 UTC
- 편집된 시간: 2017년 8월 14일, 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMacieServiceRolePolicy

`AmazonMacieServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Macie에 대한 IAM 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 19일, 22:17 UTC
- 편집된 시간: 2022년 5월 19일, 19:16 UTC

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

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonManagedBlockchainConsoleFullAccess

`AmazonManagedBlockchainConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Managed Blockchain에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonManagedBlockchainConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 4월 29일, 21:23 UTC
- 편집된 시간: 2019년 4월 29일, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess는 AWS 관리형 정책으로, Amazon Managed Blockchain에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonManagedBlockchainFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 29일, 21:39 UTC
- 편집된 시간: 2019년 4월 29일, 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonManagedBlockchainReadOnlyAccess

`AmazonManagedBlockchainReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Managed Blockchain에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonManagedBlockchainReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 30일, 18:17 UTC
- 편집된 시간: 2019년 4월 30일, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicy는 AWS 관리형 정책으로, Amazon Managed Blockchain에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 1월 17일, 19:51 UTC

- 편집된 시간: 2020년 1월 17일, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMCSFullAccess

AmazonMCSFullAccess는 AWS 관리형 정책으로, Amazon Managed Apache Cassandra Service에 대한 전체 액세스 권한 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMCSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 13:45 UTC
- 편집된 시간: 2020년 4월 17일, 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMCSReadOnlyAccess

AmazonMCSReadOnlyAccess는 AWS 관리형 정책으로, Amazon Managed Apache Cassandra Service에 대한 읽기 전용 액세스 권한 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMCSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 13:46 UTC
- 편집된 시간: 2020년 4월 17일, 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMechanicalTurkFullAccess

`AmazonMechanicalTurkFullAccess`는 AWS 관리형 정책으로, Amazon Mechanical Turk의 모든 API에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMechanicalTurkFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 11일, 19:08 UTC
- 편집된 시간: 2015년 12월 11일, 19:08 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMechanicalTurkReadOnly

`AmazonMechanicalTurkReadOnly`는 AWS 관리형 정책으로, Amazon Mechanical Turk의 읽기 전용 API에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMechanicalTurkReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 12월 11일, 19:08 UTC
- 편집된 시간: 2019년 9월 25일, 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMemoryDBFullAccess

`AmazonMemoryDBFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon MemoryDB에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMemoryDBFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 8일, 19:24 UTC
- 편집된 시간: 2021년 10월 8일, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMemoryDBReadOnlyAccess

`AmazonMemoryDBReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon MemoryDB에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMemoryDBReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 8일, 19:27 UTC

- 편집된 시간: 2021년 10월 8일, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMobileAnalyticsFinancialReportAccess

`AmazonMobileAnalyticsFinancialReportAccess`는 AWS 관리형 정책으로, 모든 애플리케이션 리소스에 대한 재무 데이터를 포함한 모든 보고서에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsFinancialReportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess는 AWS 관리형 정책으로, 모든 애플리케이션 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMobileAnalyticsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMobileAnalyticsNon-financialReportAccess

`AmazonMobileAnalyticsNon-financialReportAccess`는 AWS 관리형 정책으로, 모든 애플리케이션 리소스에 대한 비재무 보고서에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMobileAnalyticsNon-financialReportAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMobileAnalyticsWriteOnlyAccess

`AmazonMobileAnalyticsWriteOnlyAccess`는 AWS 관리형 정책으로, 모든 애플리케이션 리소스에 대한 이벤트 데이터를 넣을 수 있는 쓰기 전용 액세스를 제공합니다. (SDK 통합에 권장)

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMobileAnalyticsWriteOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMonitronFullAccess

AmazonMonitronFullAccess는 AWS 관리형 정책으로, Amazon Monitron을 관리할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMonitronFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 2일, 22:40 UTC
- 편집된 시간: 2022년 6월 8일, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMQApiFullAccess

`AmazonMQApiFullAccess`는 AWS 관리형 정책으로, API/SDK을 통해 AmazonMQ에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMQApiFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 18일, 20:31 UTC
- 편집된 시간: 2020년 11월 4일, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMQApiReadOnlyAccess

`AmazonMQApiReadOnlyAccess`는 AWS 관리형 정책으로, API/SDK을 통해 AmazonMQ에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMQApiReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 18일, 20:31 UTC
- 편집된 시간: 2018년 12월 18일, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMQFullAccess

`AmazonMQFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AmazonMQ에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMQFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 11월 28일, 15:28 UTC
- 편집된 시간: 2020년 11월 4일, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMQReadOnlyAccess

`AmazonMQReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AmazonMQ에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMQReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 11월 28일, 15:30 UTC
- 편집된 시간: 2017년 11월 28일, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicy는 AWS 관리형 정책으로, AWS Amazon MQ에 대한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 4일, 16:07 UTC
- 편집된 시간: 2020년 11월 4일, 16:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess는 AWS 관리형 정책으로, Amazon MSK Connect에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMSKConnectReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 20일, 10:18 UTC
- 편집된 시간: 2021년 10월 18일, 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMSKFullAccess

`AmazonMSKFullAccess`는 AWS 관리형 정책으로, Amazon MSK에 대한 전체 액세스 권한과 종속성에 대한 기타 필수 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonMSKFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 14일, 22:07 UTC
- 편집된 시간: 2023년 10월 18일, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess는 AWS 관리형 정책으로, Amazon MSK에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonMSKReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 14일, 22:28 UTC
- 편집된 시간: 2019년 1월 14일, 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonMWAAServiceRolePolicy

`AmazonMWAAServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Managed Workflows for Apache Airflow에서 사용하는 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 24일, 14:13 UTC
- 편집된 시간: 2022년 11월 17일, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker는 AWS 관리형 정책으로, 이 정책은 Nimble Studio Launch Profile 작업자에게 필요한 리소스에 대한 액세스를 부여합니다. 이 정책을 Nimble Studio Builder에서 생성된 EC2 인스턴스에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AmazonNimbleStudio-LaunchProfileWorker를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 28일, 04:47 UTC
- 편집된 시간: 2021년 4월 28일, 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin는 AWS 관리형 정책으로, 이 정책은 스튜디오 관리자와 연관된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스를 부여합니다. 이 정책을 스튜디오와 연관된 관리자 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AmazonNimbleStudio-StudioAdmin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 28일, 04:47 UTC
- 편집된 시간: 2023년 9월 22일, 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonNimbleStudio-StudioUser

`AmazonNimbleStudio-StudioUser`는 AWS 관리형 정책으로, 이 정책은 스튜디오 사용자와 연관된 Amazon Nimble Studio 리소스 및 다른 서비스의 관련 스튜디오 리소스에 대한 액세스를 부여합니다. 이 정책을 스튜디오와 연관된 사용자 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonNimbleStudio-StudioUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 4월 28일, 04:48 UTC
- 편집된 시간: 2023년 9월 22일, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOmicsFullAccess

`AmazonOmicsFullAccess`는 AWS 관리형 정책으로, AWS 서비스을 통해 Amazon Omics 및 기타 필요한 에 대한 전체 액세스를 제공합니다. 이 정책을 통해 사용자는 사용자의 AWS 계정 외부 리소스에 액세스하기 위한 RAM 공유 초대를 보고 수락할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOmicsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 24일, 00:59 UTC
- 편집된 시간: 2023년 2월 24일, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOmicsReadOnlyAccess

`AmazonOmicsReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Omics에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOmicsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 29일, 04:17 UTC
- 편집된 시간: 2022년 11월 29일, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOneEnterpriseFullAccess

`AmazonOneEnterpriseFullAccess`는 다음과 같은 AWS관리형 정책입니다. 이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 대한 액세스를 허용하는 관리자 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOneEnterpriseFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일 04:58 UTC
- 편집 시간: 2023년 11월 28일, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOneEnterpriseInstallerAccess

`AmazonOneEnterpriseInstallerAccess`다음과 같은 AWS관리형 정책입니다. 이 정책은 장치 설치 및 활성화를 허용하는 제한된 읽기 및 쓰기 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOneEnterpriseInstallerAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 28일 05:00 UTC
- 편집 시간: 2023년 11월 28일 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOneEnterpriseReadOnlyAccess

`AmazonOneEnterpriseReadOnlyAccess`는 다음과 같은 AWS관리형 정책입니다. 이 정책은 모든 Amazon One Enterprise 리소스 및 작업에 읽기 전용 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOneEnterpriseReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일 04:59 UTC
- 편집 시간: 2023년 11월 28일, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchDashboardsServiceRolePolicy

`AmazonOpenSearchDashboardsServiceRolePolicy`다음과 같은 AWS CloudWatch 관리형 정책으로, Amazon OpenSearch Dashboard Service에 대한 액세스를 제공하여 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있도록 합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 12월 22일 19:38 UTC
- 편집 시간: 2023년 12월 22일 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchIngestionFullAccess

`AmazonOpenSearchIngestionFullAccess`는 AWS 관리형 정책으로, Amazon OpenSearch Ingestion이 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOpenSearchIngestionFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2023년 4월 26일, 18:11 UTC
- 편집된 시간: 2023년 4월 26일, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchIngestionReadOnlyAccess

`AmazonOpenSearchIngestionReadOnlyAccess`는 AWS 관리형 정책으로, Amazon OpenSearch Ingestion Service에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOpenSearchIngestionReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 26일, 18:09 UTC
- 편집된 시간: 2023년 4월 26일, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchIngestionServiceRolePolicy

`AmazonOpenSearchIngestionServiceRolePolicy`는 AWS 관리형 정책으로, Amazon OpenSearch Ingestion Service가 사용자를 대신하여 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 18일, 16:49 UTC
- 편집된 시간: 2022년 11월 18일, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchServerlessServiceRolePolicy

`AmazonOpenSearchServerlessServiceRolePolicy`는 AWS 관리형 정책으로, Amazon OpenSearch Serverless가 사용자를 대신하여 CloudWatch API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 24일, 19:50 UTC
- 편집된 시간: 2022년 11월 24일, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess는 AWS 관리형 정책으로, Amazon Cognito 구성 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchServiceCognitoAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 2일, 06:31 UTC
- 편집된 시간: 2021년 12월 20일, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchServiceFullAccess

`AmazonOpenSearchServiceFullAccess`는 AWS 관리형 정책으로, Amazon OpenSearch Service 구성 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonOpenSearchServiceFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2021년 9월 8일, 05:33 UTC
- 편집된 시간: 2021년 9월 8일, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchServiceReadOnlyAccess

`AmazonOpenSearchServiceReadOnlyAccess`는 AWS 관리형 정책으로, Amazon OpenSearch Service 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonOpenSearchServiceReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 8일, 05:38 UTC
- 편집된 시간: 2021년 9월 8일, 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonOpenSearchServiceRolePolicy

AmazonOpenSearchServiceRolePolicy는 AWS 관리형 정책으로, Amazon OpenSearch Service가 사용자를 대신하여 EC2 네트워킹 API와 같은 다른 AWS 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 26일, 09:27 UTC
- 편집된 시간: 2023년 10월 23일, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
```

```
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPersonalizeFullAccess

`AmazonPersonalizeFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Amazon Personalize에 대한 전체 액세스를 제공합니다. 또한 관련 서비스(예: S3, CloudWatch)에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonPersonalizeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 12월 4일, 22:24 UTC
- 편집된 시간: 2019년 5월 30일, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPollyFullAccess

AmazonPollyFullAccess는 AWS 관리형 정책으로, Amazon Polly 서비스 및 리소스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonPollyFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 18:59 UTC
- 편집된 시간: 2016년 11월 30일, 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPollyReadOnlyAccess

`AmazonPollyReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Polly 리소스에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonPollyReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 18:59 UTC
- 편집된 시간: 2018년 7월 17일, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPrometheusConsoleFullAccess

AmazonPrometheusConsoleFullAccess는 AWS 관리형 정책으로, AWS 콘솔의 AWS Managed Prometheus 리소스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:11 UTC
- 편집된 시간: 2022년 10월 24일, 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPrometheusFullAccess

AmazonPrometheusFullAccess는 AWS 관리형 정책으로, AWS Managed Prometheus 리소스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:10 UTC
- 편집 시간: 2023년 11월 26일 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPrometheusQueryAccess

AmazonPrometheusQueryAccess는 AWS 관리형 정책으로, AWS Managed Prometheus 리소스에 대해 쿼리를 실행할 수 있는 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonPrometheusQueryAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 19일, 01:02 UTC
- 편집된 시간: 2020년 12월 19일, 01:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPrometheusRemoteWriteAccess

`AmazonPrometheusRemoteWriteAccess`는 AWS 관리형 정책으로, AWS Managed Prometheus workspaces에 대한 쓰기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonPrometheusRemoteWriteAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 19일, 01:04 UTC
- 편집된 시간: 2020년 12월 19일, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonPrometheusScraperServiceRolePolicy

`AmazonPrometheusScraperServiceRolePolicy`AWSPrometheus Collector용 Amazon 관리형 서비스에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공하는 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 26일, 14:19 UTC
- 편집 시간: 2023년 11월 26일, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*: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:*:eks:*:*:cluster/*"
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:*:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonQFullAccess

AmazonQFullAccessAmazon Q와의 상호 작용을 가능하게 하는 전체 액세스 권한을 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 28일, 16:00 UTC
- 편집 시간: 2023년 11월 28일 16:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonQLDBConsoleFullAccess

`AmazonQLDBConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon QLDB에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonQLDBConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:24 UTC
- 편집된 시간: 2022년 11월 4일, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonQLDBFullAccess

AmazonQLDBFullAccess는 AWS 관리형 정책으로, 서비스 API를 통해 Amazon QLDB에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQLDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:23 UTC
- 편집된 시간: 2022년 11월 4일, 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonQLDBReadOnly

AmazonQLDBReadOnly는 AWS 관리형 정책으로, Amazon QLDB에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonQLDBReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 9월 5일, 18:19 UTC
- 편집된 시간: 2021년 7월 2일, 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSBetaServiceRolePolicy

AmazonRDSBetaServiceRolePolicy는 AWS 관리형 정책으로, Amazon RDS가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 2일, 19:41 UTC
- 편집된 시간: 2022년 12월 14일, 18:33 UTC

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

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
```

```
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicyAmazon RDS Custom이 EC2 인스턴스 프로필을 통해 다양한 자동화 작업 및 데이터베이스 관리 작업을 수행할 수 있도록 허용하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSCustomInstanceProfileRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 작성 시간: 2024년 2월 27일 17:42 UTC
- 편집 시간: 2024년 2월 27일 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:do-
not-delete-rds-custom-*"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRDSCustomPreviewServiceRolePolicy

`AmazonRDSCustomPreviewServiceRolePolicy`는 AWS 관리형 정책으로, Amazon RDS Custom 프리뷰 서비스 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 8일, 21:44 UTC
- 편집된 시간: 2023년 9월 20일, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
```

```
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy는 AWS 관리형 정책으로, Amazon RDS Custom이 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 8일, 21:39 UTC
- 편집된 시간: 2023년 9월 20일, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
```

```
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
```

```
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
```

```
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
```

```
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSDataFullAccess

AmazonRDSDataFullAccess는 AWS 관리형 정책으로, RDS 데이터 API, RDS 데이터베이스 보안 인증 정보를 위한 비밀 저장소 API, DB 콘솔 쿼리 관리 API를 사용하여 AWS 계정의 Aurora Serverless 클러스터에서 SQL 문을 실행할 수 있는 전체 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSDataFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 20일, 21:29 UTC
- 편집된 시간: 2019년 11월 20일, 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSDataFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSDirectoryServiceAccess

`AmazonRDSDirectoryServiceAccess`는 AWS 관리형 정책으로, RDS가 도메인에 가입된 SQL Server DB 인스턴스에 대해 고객을 대신하여 Directory Service Managed AD에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRDSDirectoryServiceAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 26일, 02:02 UTC
- 편집된 시간: 2019년 5월 15일, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSEnhancedMonitoringRole

`AmazonRDSEnhancedMonitoringRole`는 AWS 관리형 정책으로, RDS Enhanced Monitoring을 위해 Cloudwatch에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRDSEnhancedMonitoringRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 11일, 19:58 UTC
- 편집된 시간: 2015년 11월 11일, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSFullAccess

`AmazonRDSFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon RDS에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRDSFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 8월 17일, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSPerformanceInsightsFullAccess

`AmazonRDSPerformanceInsightsFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 RDS Performance Insights에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRDSPerformanceInsightsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 15일, 23:41 UTC
- 편집된 시간: 2023년 10월 23일, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSPerformanceInsightsReadOnly

`AmazonRDSPerformanceInsightsReadOnly`는 AWS 관리형 정책으로, RDS Performance Insights에 대한 읽기 전용 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRDSPerformanceInsightsReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 5일, 00:02 UTC
- 편집된 시간: 2023년 10월 23일, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy는 AWS 관리형 정책으로, Amazon RDS 프리뷰 서비스 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 31일, 18:02 UTC
- 편집된 시간: 2023년 10월 4일, 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon RDS에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRDSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 4월 14일, 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRDSServiceRolePolicy

AmazonRDSServiceRolePolicy는 AWS 관리형 정책으로, Amazon RDS가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 1월 8일, 18:17 UTC
- 편집 시간: 2024년 1월 19일 15:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Sns",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
```

```
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
```

```
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRedshiftAllCommandsFullAccess

`AmazonRedshiftAllCommandsFullAccess`는 AWS 관리형 정책으로, 이 정책에는 Amazon Redshift에서 데이터를 복사, 로드, 언로드, 쿼리 및 분석하기 위한 SQL 명령을 실행할 수 있는 권한이 포함되어 있습니다. 이 정책은 Amazon S3, Amazon CloudWatch Logs, Amazon SageMaker 및 AWS Glue와 같은 관련 서비스에 대해 select 문을 실행할 수 있는 권한도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftAllCommandsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 4일, 00:48 UTC
- 편집된 시간: 2021년 11월 25일, 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess는 AWS 관리형 정책으로, 이 정책은 Amazon Redshift Data API에 대한 전체 액세스를 제공합니다. 이 정책은 다른 필수 서비스에 대한 범위 지정된 액세스 권한도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftDataFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 9일, 19:23 UTC
- 편집된 시간: 2023년 4월 7일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRedshiftFullAccess

`AmazonRedshiftFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon Redshift에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRedshiftFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2022년 7월 7일, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRedshiftQueryEditor

`AmazonRedshiftQueryEditor`는 AWS 관리형 정책으로, Amazon Redshift 쿼리 에디터 및 AWS Management Console를 통해 저장된 쿼리에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRedshiftQueryEditor`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 4일, 22:50 UTC
- 편집된 시간: 2021년 2월 16일, 19:33 UTC

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

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRedshiftQueryEditorV2FullAccess

`AmazonRedshiftQueryEditorV2FullAccess`는 AWS 관리형 정책으로, Amazon Redshift 쿼리 에디터 V2 작업 및 리소스에 대한 전체 액세스를 부여합니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고, AWS KMS에서 키와 별칭을 읽고, Secrets Manager에서 쿼리 편집기 V2 비밀을 관리할 수 있는 권한이 포함됩니다. AWS

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRedshiftQueryEditorV2FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2021년 9월 24일, 14:06 UTC
- 편집 시간: 2024년 2월 21일 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRedshiftQueryEditorV2NoSharing

`AmazonRedshiftQueryEditorV2NoSharing`은 AWS 관리형 정책으로, 리소스를 공유하지 않고 Amazon Redshift 쿼리 에디터 V2로 작업할 수 있는 기능을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 업데이트하고, 삭제할 수만 있고 공유할 수는 없습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRedshiftQueryEditorV2NoSharing`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:18 UTC
- 편집 시간: 2024년 2월 21일 17:25 UTC

- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRedshiftQueryEditorV2ReadSharing

AmazonRedshiftQueryEditorV2ReadSharing는 AWS 관리형 정책으로, 제한된 리소스 공유로 Amazon Redshift 쿼리 에디터 V2로 작업할 수 있는 권한을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 쓰고, 공유할 수 있습니다. 부여된 보안 주체는 팀과 공유된 리소스를 읽을 수 있지만 업데이트할 수는 없습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2ReadSharing를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:22 UTC
- 편집 시간: 2024년 2월 21일 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRedshiftQueryEditorV2ReadWriteSharing

`AmazonRedshiftQueryEditorV2ReadWriteSharing`는 AWS 관리형 정책으로, 리소스 공유를 통해 Amazon Redshift 쿼리 에디터 V2로 작업할 수 있는 권한을 부여합니다. 부여된 보안 주체는 자신의 리소스를 읽고, 쓰고, 공유할 수 있습니다. 부여된 보안 주체는 팀과 공유하는 리소스를 읽고 업데이트할 수 있습니다. 이 정책은 다른 필수 서비스에 대한 액세스 권한도 부여합니다. 여기에는 Amazon Redshift 클러스터를 나열하고 Secrets Manager에서 AWS 보안 주체의 쿼리 편집기 V2 암호를 관리할 수 있는 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRedshiftQueryEditorV2ReadWriteSharing를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 24일, 14:25 UTC
- 편집 시간: 2024년 2월 21일 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRedshiftReadOnlyAccess

`AmazonRedshiftReadOnlyAccess`는 다음을 통해 Amazon Redshift에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRedshiftReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2024년 2월 8일 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRedshiftServiceLinkedRolePolicy

`AmazonRedshiftServiceLinkedRolePolicy`다음과 같은 AWS 관리형 정책입니다. Amazon Redshift가 사용자를 대신하여 AWS 서비스를 호출하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 18일, 19:19 UTC
- 편집 시간: 2024년 3월 15일 20:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonRekognitionCustomLabelsFullAccess

`AmazonRekognitionCustomLabelsFullAccess`는 AWS 관리형 정책으로, 이 정책은 Amazon Rekognition Custom Labels 기능에 필요한 rekognition 및 s3 권한을 지정합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRekognitionCustomLabelsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 8일, 19:18 UTC
- 편집된 시간: 2022년 8월 16일, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRekognitionFullAccess

`AmazonRekognitionFullAccess`는 AWS 관리형 정책으로, 모든 Amazon Rekognition API에 대한 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRekognitionFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 30일, 14:40 UTC
- 편집된 시간: 2016년 11월 30일, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRekognitionReadOnlyAccess

`AmazonRekognitionReadOnlyAccess`는 AWS 관리형 정책으로, 모든 Read rekognition API에 대한 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRekognitionReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2016년 11월 30일, 14:58 UTC
- 편집된 시간: 2023년 11월 8일, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRekognitionServiceRole

AmazonRekognitionServiceRole는 AWS 관리형 정책으로, Rekognition이 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRekognitionServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2017년 11월 29일, 16:52 UTC
- 편집된 시간: 2017년 11월 29일, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53AutoNamingFullAccess

`AmazonRoute53AutoNamingFullAccess`는 AWS 관리형 정책으로, 모든 Route 53 Auto Naming 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53AutoNamingFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 1월 18일, 18:40 UTC
- 편집된 시간: 2018년 1월 18일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53AutoNamingReadOnlyAccess

`AmazonRoute53AutoNamingReadOnlyAccess`는 AWS 관리형 정책으로, 모든 Route 53 Auto Naming 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53AutoNamingReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 1월 18일, 03:02 UTC
- 편집된 시간: 2018년 1월 18일, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess는 AWS 관리형 정책으로, Route 53 Auto Naming 작업에 대한 등록자 수준 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53AutoNamingRegistrantAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 12일, 22:33 UTC
- 편집된 시간: 2018년 3월 12일, 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53DomainsFullAccess

`AmazonRoute53DomainsFullAccess`는 AWS 관리형 정책으로, 도메인 등록의 일부로 Hosted Zone 생성을 허용하기 위해 모든 Route53 Domains 작업 및 Create Hosted Zone에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53DomainsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess`는 AWS 관리형 정책으로, Route53 Domains 목록 및 작업에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53DomainsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53FullAccess

`AmazonRoute53FullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 Amazon Route 53에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2018년 12월 20일, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 Amazon Route 53에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2016년 11월 15일, 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryClusterFullAccess

`AmazonRoute53RecoveryClusterFullAccess`는 AWS 관리형 정책으로, Amazon Route 53 Recovery Cluster에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53RecoveryClusterFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:37 UTC
- 편집된 시간: 2021년 8월 18일, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryClusterReadOnlyAccess

`AmazonRoute53RecoveryClusterReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Route 53 Recovery Cluster에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53RecoveryClusterReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 17:36 UTC
- 편집된 시간: 2022년 4월 1일, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryControlConfigFullAccess

`AmazonRoute53RecoveryControlConfigFullAccess`는 AWS 관리형 정책으로, Amazon Route 53 Recovery Control Config에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53RecoveryControlConfigFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 17:48 UTC
- 편집된 시간: 2021년 8월 18일, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryControlConfigReadOnlyAccess

AmazonRoute53RecoveryControlConfigReadOnlyAccess는 AWS 관리형 정책으로, Amazon Route 53 Recovery Control Config에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53RecoveryControlConfigReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:01 UTC
- 편집된 시간: 2023년 10월 18일, 17:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryReadinessFullAccess

`AmazonRoute53RecoveryReadinessFullAccess`는 AWS 관리형 정책으로, Amazon Route 53 Recovery Readiness에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53RecoveryReadinessFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 16:45 UTC
- 편집된 시간: 2021년 8월 18일, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53RecoveryReadinessReadOnlyAccess

`AmazonRoute53RecoveryReadinessReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Route 53 Recovery Readiness에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53RecoveryReadinessReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 18일, 18:11 UTC
- 편집된 시간: 2021년 11월 9일, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess`는 AWS 관리형 정책으로, Route 53 Resolver에 대한 전체 액세스 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonRoute53ResolverFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 30일, 18:10 UTC
- 편집된 시간: 2020년 7월 17일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess는 AWS 관리형 정책으로, Route 53 Resolver에 대한 읽기 전용 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonRoute53ResolverReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 30일, 18:11 UTC
- 편집된 시간: 2019년 9월 27일, 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonS3FullAccess

`AmazonS3FullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 버킷에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonS3FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2021년 9월 27일, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy는 AWS 관리형 정책으로, Amazon S3 객체 Lambda와 상호 작용할 수 있는 AWS Lambda 함수 권한을 제공합니다. 또한 CloudWatch Logs에 쓸 수 있는 Lambda 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3ObjectLambdaExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 8월 18일, 10:07 UTC

- 편집된 시간: 2021년 8월 18일, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonS3OutpostsFullAccess

AmazonS3OutpostsFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon S3 on Outposts에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonS3OutpostsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 2일, 17:26 UTC
- 편집된 시간: 2020년 10월 2일, 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonS3OutpostsReadOnlyAccess

`AmazonS3OutpostsReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon S3 on Outposts에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonS3OutpostsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 2일, 18:55 UTC
- 편집된 시간: 2020년 10월 2일, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonS3ReadOnlyAccess

`AmazonS3ReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 모든 버킷에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonS3ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC

- 편집된 시간: 2023년 8월 10일, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy는 AWS 관리형 정책으로, AWS 서비스 Catalog 서비스에서 Amazon SageMaker 제품 포트폴리오의 제품을 프로비저닝하는 데 사용되는 서비스 역할 정책입니다. CodePipeline, CodeBuild, CodeCommit, Glue, CloudFormation 등을 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 27일, 18:48 UTC
- 편집된 시간: 2022년 8월 2일, 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
```

```
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
```

```
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
```

```
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
```

```
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasAIServicesAccess

AmazonSageMakerCanvasAIServicesAccess는 Amazon SageMaker Canvas가 AI 서비스를 사용하여 바로 사용할 수 있는 AI 솔루션을 지원할 수 있는 권한을 제공하는 AWS관리형 정책입니다. Amazon SageMaker Canvas가 지원을 추가함에 따라 이 정책은 서비스에 대한 변경 권한을 더 추가합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasAIServicesAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 23일, 22:36 UTC
- 편집 시간: 2023년 11월 29일 14:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccess다음과 같은 AWS관리형 정책입니다. 이 정책은 S3와 같은 다운스트림 서비스에 대한 액세스를 제공하여 Amazon Bedrock in SageMaker Canvas를 사용할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasBedrockAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2024년 2월 2일 18:37 UTC
- 편집 시간: 2024년 2월 2일 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasDataPrepFullAccess

`AmazonSageMakerCanvasDataPrepFullAccess`Canvas에서의 데이터 준비를 위해 Amazon SageMaker 리소스 및 작업에 대한 전체 액세스 권한을 제공하는 AWS관리형 정책입니다. 이 정책은 또한 관련 서비스 (예: S3, IAM, KMS, RDS, 로그, Redshift, Athena, Glue, CloudWatch , Secrets Manager) 에 대한 선택적 액세스를 제공합니다. EventBridge 이 정책은 Amazon SageMaker 도메인/사용자 프로필 실행 역할에 연결되어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerCanvasDataPrepFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 10월 27일, 22:56 UTC

- 편집 시간: 2023년 12월 8일 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccess는 AWS 관리형 정책으로, Amazon SageMaker Canvas가 Canvas를 통해 생성된 엔드포인트에 대한 엔드포인트 세부 정보를 생성, 관리 및 확인할 수 있도록 허용합니다. Amazon SageMaker Canvas가 CloudWatch에서 엔드포인트 호출 지표를 검색할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasDirectDeployAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 6일, 18:11 UTC
- 편집된 시간: 2023년 10월 6일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccess는 AWS 관리형 정책으로, 이 정책은 SageMaker Canvas를 Amazon Forecast와 함께 사용하는 데 일반적으로 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerCanvasForecastAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 8월 24일, 20:04 UTC
- 편집된 시간: 2022년 8월 24일, 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCanvasFullAccess

`AmazonSageMakerCanvasFullAccess`Amazon SageMaker Canvas 리소스 및 작업에 대한 전체 액세스를 제공하는 AWS관리형 정책입니다. 또한 이 정책은 관련 서비스 (예: S3, IAM, VPC, ECR, CloudWatch 로그, Redshift, Secrets Manager 및 Forecast) 에 대한 선택적 액세스를 제공합니다. 이 정책은 Amazon SageMaker 도메인/사용자 프로필 실행 역할에 연결되어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerCanvasFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 9월 9일, 00:44 UTC
- 편집 시간: 2024년 1월 24일 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
```

```
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
```

```
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
```

```
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
```

```
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
 "sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerClusterInstanceRolePolicy

`AmazonSageMakerClusterInstanceRolePolicy`는 다음과 같은 AWS관리형 정책입니다. 이 정책은 Amazon SageMaker Cluster를 사용하는 데 일반적으로 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerClusterInstanceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 29일 15:11 UTC
- 편집 시간: 2023년 11월 29일 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker Core Services의 서비스 연결 역할에 대한 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 21일, 21:40 UTC
- 편집된 시간: 2020년 12월 21일, 21:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy는 AWS 관리형 정책으로, SageMaker Edge가 기본 클라우드 연결을 사용하여 고객을 위한 장치 플릿을 생성하고 관리하는 데 필요한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerEdgeDeviceFleetPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 8일, 16:17 UTC
- 편집된 시간: 2020년 12월 8일, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerFeatureStoreAccess

`AmazonSageMakerFeatureStoreAccess`는 AWS 관리형 정책으로, Amazon SageMaker FeatureStore 기능 그룹에 대한 오프라인 저장소를 활성화하는 데 필요한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerFeatureStoreAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 16:24 UTC
- 편집된 시간: 2022년 12월 5일, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerFullAccess

`AmazonSageMakerFullAccess`AWS Management Console및 SDK를 SageMaker 통해 Amazon에 대한 전체 액세스 권한을 제공하는 AWS관리형 정책입니다. 또한 관련 서비스 (예: S3, ECR, CloudWatch 로그) 에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 13:07 UTC
- 편집 시간: 2023년 11월 30일 13:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

정책 버전

정책 버전: v25(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
```

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

```
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
```

```
            "codecommit:List*",
            "cognito-idp:AdminAddUserToGroup",
            "cognito-idp:AdminCreateUser",
            "cognito-idp:AdminDeleteUser",
            "cognito-idp:AdminDisableUser",
            "cognito-idp:AdminEnableUser",
            "cognito-idp:AdminRemoveUserFromGroup",
            "cognito-idp:CreateGroup",
            "cognito-idp:CreateUserPool",
            "cognito-idp:CreateUserPoolClient",
            "cognito-idp:CreateUserPoolDomain",
            "cognito-idp:DescribeUserPool",
            "cognito-idp:DescribeUserPoolClient",
            "cognito-idp:List*",
            "cognito-idp:UpdateUserPool",
            "cognito-idp:UpdateUserPoolClient",
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcs",
            "ecr:BatchCheckLayerAvailability",
            "ecr:BatchGetImage",
            "ecr:CreateRepository",
            "ecr:Describe*",
            "ecr:GetAuthorizationToken",
            "ecr:GetDownloadUrlForLayer",
            "ecr:StartImageScan",
            "elastic-inference:Connect",
            "elasticfilesystem:DescribeFileSystems",
            "elasticfilesystem:DescribeMountTargets",
            "fsx:DescribeFileSystems",
            "glue:CreateJob",
            "glue:DeleteJob",
            "glue:GetJob*",
            "glue:GetTable*",
            "glue:GetWorkflowRun",
```

```
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
```

```
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
```

```
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
```

```
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
```

```
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerGeospatialExecutionRole

`AmazonSageMakerGeospatialExecutionRole`는 AWS 관리형 정책으로, 이 정책은 SageMaker 지리 공간을 사용하는 데 일반적으로 필요한 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerGeospatialExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 11월 30일, 10:08 UTC
- 편집된 시간: 2023년 5월 10일, 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerGeospatialFullAccess

`AmazonSageMakerGeospatialFullAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Management Console 및 SDK를 통해 Amazon SageMaker Geospatial에 대한 전체 액세스를 허용하는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerGeospatialFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 11월 30일, 10:06 UTC
- 편집된 시간: 2022년 11월 30일, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution는 AWS 관리형 정책으로, SageMaker GroundTruth Labeling 작업을 실행하는 데 필요한 AWS 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerGroundTruthExecution를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 9일, 19:30 UTC
- 편집된 시간: 2022년 4월 29일, 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerMechanicalTurkAccess

`AmazonSageMakerMechanicalTurkAccess`는 AWS 관리형 정책으로, 모든 Workteam을 대상으로 Amazon Augmented AI FlowDefinition 리소스를 생성할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerMechanicalTurkAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 16:19 UTC
- 편집된 시간: 2019년 12월 3일, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerModelGovernanceUseAccess

AmazonSageMakerModelGovernanceUseAccess는 AWS 관리형 정책으로, 모든 Amazon SageMaker Governance 기능을 사용하는 데 필요한 권한을 부여하는 AWS 관리형 정책입니다. 또한 이 정책은 관련 서비스(예: S3, KMS)에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerModelGovernanceUseAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 30일, 08:58 UTC
- 편집된 시간: 2023년 7월 17일, 22:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
```

```
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccess는 AWS 관리형 정책으로, Sagemaker의 Model Registry에 대한 새로운 관리형 정책입니다. 이 정책은 사용자 역할에 연결하여 Sagemaker의 Model Registry 관련 기능에 액세스할 수 있는 독립형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerModelRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 13일, 05:20 UTC
- 편집된 시간: 2023년 4월 13일, 05:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerNotebooksServiceRolePolicy

`AmazonSageMakerNotebooksServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker Notebooks의 서비스 연결 역할에 대한 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 18일, 20:27 UTC
- 편집된 시간: 2023년 3월 9일, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS API Gateway가 사용하는 서비스 역할 정책입니다. Lambda 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:06 UTC
- 편집된 시간: 2023년 8월 1일, 15:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServ

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS CloudFormation이 사용하는 서비스 역할 정책입니다. Lambda, APIGateway 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:06 UTC
- 편집된 시간: 2023년 8월 1일, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS Lambda가 사용하는 서비스 역할 정책입니다. Secrets Manager 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 8월 1일, 15:05 UTC
- 편집된 시간: 2023년 8월 1일, 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerPipelinesIntegrations

`AmazonSageMakerPipelinesIntegrations`는 AWS 관리형 정책으로, SageMaker Model Building Pipelines의 Callback 단계 및 Lambda 단계에서 사용하는 데 일반적으로 필요한 권한을 부여하는 Amazon 관리형 정책입니다. 이는 SageMaker Studio를 설정할 때 생성할 수 있는 AmazonSageMaker-ExecutionRole에 추가됩니다. 또한 파이프라인을 작성하거나 실행하는 데 사용되는 다른 모든 역할에 연결할 수도 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerPipelinesIntegrations`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 7월 30일, 16:35 UTC
- 편집된 시간: 2023년 2월 17일, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerReadOnly

`AmazonSageMakerReadOnly`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 Amazon SageMaker에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 13:07 UTC
- 편집된 시간: 2021년 12월 1일, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS API Gateway가 사용하는 서비스 역할 정책입니다. CloudWatch Logs 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 3월 25일, 04:25 UTC
- 편집된 시간: 2022년 3월 25일, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS CloudFormation이 사용하는 서비스 역할 정책입니다. SageMaker 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 3월 25일, 04:26 UTC
- 편집된 시간: 2022년 3월 25일, 04:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS CodeBuild가 사용하는 서비스 역할 정책입니다. CodePipeline, CodeBuild 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 3월 25일, 04:27 UTC
- 편집된 시간: 2022년 3월 25일, 04:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
```

```
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
```

```
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
```

```
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
```

```
            "sagemaker:ListAlgorithms",
            "sagemaker:ListAppImageConfigs",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListCompilationJobs",
            "sagemaker:ListContexts",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDevices",
            "sagemaker:ListDomains",
            "sagemaker:ListEdgePackagingJobs",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListExperiments",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHumanLoops",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListImages",
            "sagemaker:ListInferenceRecommendationsJobs",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListLabelingJobsForWorkteam",
            "sagemaker:ListLineageGroups",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringExecutions",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
```

```
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
```

```
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS CodePipeline이 사용하는 서비스 역할 정책입니다. CodePipeline, CodeBuild 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:53 UTC
- 편집된 시간: 2022년 2월 22일, 09:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS CloudWatch Events가 사용하는 서비스 역할 정책입니다. CodePipeline 등을 포함한 관련 서비스의 서브셋에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:53 UTC

- 편집된 시간: 2022년 2월 22일, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서

AWS Firehose가 사용하는 서비스 역할 정책입니다. Firehose 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:54 UTC
- 편집된 시간: 2022년 2월 22일, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS Glue가 사용하는 서비스 역할 정책입니다. Glue, S3 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 2월 22일, 09:51 UTC
- 편집된 시간: 2022년 8월 26일, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker 제품 포트폴리오의 AWS ServiceCatalog 프로비저닝 제품 내에서 AWS Lambda가 사용하는 서비스 역할 정책입니다. ECR, S3 및 기타 서비스를 포함한 관련 서비스 세트에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 4일, 16:34 UTC
- 편집된 시간: 2022년 4월 4일, 16:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
```

```
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
```

```
            "sagemaker:CreateCompilationJob",
            "sagemaker:CreateContext",
            "sagemaker:CreateDataQualityJobDefinition",
            "sagemaker:CreateDeviceFleet",
            "sagemaker:CreateDomain",
            "sagemaker:CreateEdgePackagingJob",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateExperiment",
            "sagemaker:CreateFeatureGroup",
            "sagemaker:CreateFlowDefinition",
            "sagemaker:CreateHumanTaskUi",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateImage",
            "sagemaker:CreateImageVersion",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateLabelingJob",
            "sagemaker:CreateLineageGroupPolicy",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelBiasJobDefinition",
            "sagemaker:CreateModelExplainabilityJobDefinition",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreateModelQualityJobDefinition",
            "sagemaker:CreateMonitoringSchedule",
            "sagemaker:CreateNotebookInstance",
            "sagemaker:CreateNotebookInstanceLifecycleConfig",
            "sagemaker:CreatePipeline",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreatePresignedNotebookInstanceUrl",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateProject",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateTrial",
            "sagemaker:CreateTrialComponent",
            "sagemaker:CreateUserProfile",
            "sagemaker:CreateWorkforce",
            "sagemaker:CreateWorkteam",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteAlgorithm",
            "sagemaker:DeleteApp",
            "sagemaker:DeleteAppImageConfig",
            "sagemaker:DeleteArtifact",
```

```
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
```

```
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
```

```
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
```

```
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
```

```
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
```

```
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSecurityLakeAdministrator

`AmazonSecurityLakeAdministrator`는 AWS 관리형 정책으로, Security Lake를 관리하는 데 필요한 Amazon Security Lake 및 관련 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSecurityLakeAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 30일, 22:04 UTC
- 편집 시간: 2024년 2월 23일 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonSecurityLakeMetastoreManager

`AmazonSecurityLakeMetastoreManager`다음과 같은 AWS관리형 정책입니다. 클라우드워치, S3, Glue 및 SQS에 대한 액세스를 허용하는 Amazon SecurityLake 메타 스토어 관리자 람다에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSecurityLakeMetastoreManager를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2024년 1월 23일 15:26 UTC
- 편집 시간: 2024년 1월 23일 15:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSecurityLakePermissionsBoundary

`AmazonSecurityLakePermissionsBoundary`는 AWS 관리형 정책으로, Amazon Security Lake는 타사 사용자 지정 소스가 데이터 레이크에 데이터를 기록하고 타사 구독자가 데이터 레이크의 데이터를 소비하도록 IAM 역할을 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSecurityLakePermissionsBoundary`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 29일, 14:11 UTC
- 편집된 시간: 2022년 11월 29일, 14:11 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
```

```
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Effect" : "Deny",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
```

```
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSESFullAccess

`AmazonSESFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SES에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSESFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSESReadOnlyAccess

`AmazonSESReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SES에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSESReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSNSFullAccess

`AmazonSNSFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SNS에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSNSReadOnlyAccess

AmazonSNSReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SNS에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSNSRole

AmazonSNSRole는 AWS 관리형 정책으로, Amazon SNS 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSNSRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSQSFullAccess

`AmazonSQSFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SQS에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSQSFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSQSReadOnlyAccess

`AmazonSQSReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon SQS에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSQSReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2023년 6월 15일, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess는 AWS 관리형 정책으로, 자동화 실행을 보고 승인 대기 중인 자동화에 승인 결정을 전송할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMAutomationApproverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 7일, 23:07 UTC
- 편집된 시간: 2017년 8월 7일, 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMAutomationRole

AmazonSSMAutomationRole는 AWS 관리형 정책으로, EC2 Automation 서비스가 자동화 문서에 정의된 활동을 실행할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMAutomationRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 5일, 22:09 UTC
- 편집된 시간: 2017년 7월 24일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMDirectoryServiceAccess

`AmazonSSMDirectoryServiceAccess`는 AWS 관리형 정책으로, 이 정책은 SSM Agent가 관리형 인스턴스에 도메인에 가입을 위해 고객을 대신하여 Directory Service에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSSMDirectoryServiceAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 3월 15일, 17:44 UTC
- 편집된 시간: 2019년 3월 15일, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMFullAccess

AmazonSSMFullAccess는 AWS 관리형 정책으로, Amazon SSM에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 29일, 17:39 UTC
- 편집된 시간: 2019년 11월 20일, 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole는 AWS 관리형 정책으로, EC2 유지 관리 기간에 사용될 서비스 역할입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSSMMaintenanceWindowRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 1일, 15:57 UTC
- 편집된 시간: 2019년 7월 27일, 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMManagedEC2InstanceDefaultPolicy

`AmazonSSMManagedEC2InstanceDefaultPolicy`는 AWS 관리형 정책으로, 이 정책은 EC2 인스턴스에서 AWS Systems Manager 기능을 활성화합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSSMManagedEC2InstanceDefaultPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 30일, 20:54 UTC
- 편집된 시간: 2022년 8월 30일, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMManagedInstanceCore

`AmazonSSMManagedInstanceCore`는 AWS 관리형 정책으로, AWS Systems Manager 서비스 핵심 기능을 활성화하기 위한 Amazon EC2 역할 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSSMManagedInstanceCore`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 3월 15일, 17:22 UTC
- 편집된 시간: 2019년 5월 23일, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMPatchAssociation

`AmazonSSMPatchAssociation`은 AWS 관리형 정책으로, 패치 연결 작업을 위해 하위 인스턴스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSSMPatchAssociation`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 13일, 16:00 UTC
- 편집된 시간: 2020년 5월 13일, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMReadOnlyAccess

`AmazonSSMReadOnlyAccess`는 AWS 관리형 정책으로, Amazon SSM에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonSSMReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 29일, 17:44 UTC
- 편집된 시간: 2015년 5월 29일, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy는 AWS 관리형 정책으로, Amazon SSM에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 13일, 19:20 UTC
- 편집된 시간: 2022년 9월 14일, 19:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonSumerianFullAccess

`AmazonSumerianFullAccess`는 AWS 관리형 정책으로, Amazon Sumerian에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonSumerianFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 24일, 20:14 UTC
- 편집된 시간: 2018년 4월 24일, 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTextractFullAccess

AmazonTextractFullAccess는 AWS 관리형 정책으로, 모든 Amazon Textract API에 대한 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTextractFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 19:07 UTC
- 편집된 시간: 2018년 11월 28일, 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTextractServiceRole

`AmazonTextractServiceRole`는 AWS 관리형 정책으로, Textract이 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonTextractServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 28일, 19:12 UTC
- 편집된 시간: 2018년 11월 28일, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTimestreamConsoleFullAccess

AmazonTimestreamConsoleFullAccess는 AWS 관리형 정책으로, AWS Management Console을 사용하여 Amazon Timestream을 관리할 수 있는 전체 액세스를 제공합니다. 참고로 이 정책은 특정 KMS 작업 및 저장된 쿼리를 관리하는 작업에 대한 권한도 부여합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2022년 2월 1일, 21:37 UTC

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

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTimestreamFullAccess

AmazonTimestreamFullAccess는 AWS 관리형 정책으로, Amazon Timestream에 대한 전체 액세스를 제공합니다. 참고로 이 정책은 특정 KMS 작업 액세스 권한도 부여합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2021년 11월 26일, 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccessAmazon Timestream InfluxDB 인스턴스를 생성, 업데이트, 삭제 및 나열하고 파라미터 그룹을 생성 및 나열할 수 있는 전체 관리 액세스 권한을 제공하는 AWS 관리형 정책입니다. 필요한 추가 권한은 설명서를 참조하십시오.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamInfluxDBFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 3월 14일 22:53 UTC
- 편집 시간: 2024년 3월 14일 22:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
```

```
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonTimestreamInfluxDBServiceRolePolicy

`AmazonTimestreamInfluxDBServiceRolePolicy`Amazon Timestream InfluxDB 인스턴스를 생성, 업데이트, 삭제 및 나열하고 파라미터 그룹을 생성 및 나열할 수 있는 전체 관리 액세스 권한을 제공하는 AWS 관리형 정책입니다. 필요한 추가 권한은 설명서를 참조하십시오.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2024년 3월 14일 18:53 UTC
- 편집 시간: 2024년 3월 14일 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess는 AWS 관리형 정책으로, Amazon Timestream에 대한 읽기 전용 액세스를 제공합니다. 정책은 실행 중인 모든 쿼리를 취소할 수 있는 권한도 제공합니다. 고객 관리형 CMK를 사용하는 경우 필요한 추가 권한은 설명서를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 AmazonTimestreamReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2023년 2월 28일, 18:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTranscribeFullAccess

`AmazonTranscribeFullAccess`는 AWS 관리형 정책으로, Amazon Transcribe 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonTranscribeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 4일, 16:06 UTC
- 편집된 시간: 2018년 4월 4일, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonTranscribeReadOnlyAccess

`AmazonTranscribeReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Transcribe에 대한 읽기 전용 작업에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonTranscribeReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 4월 4일, 16:05 UTC
- 편집된 시간: 2018년 4월 4일, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations는 AWS 관리형 정책으로, 네트워크 인터페이스를 생성하여 교차 계정 리소스에 연결할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonVPCCrossAccountNetworkInterfaceOperations를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 7월 18일, 20:47 UTC
- 편집된 시간: 2023년 9월 25일, 15:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonVPCFullAccess

`AmazonVPCFullAccess`는 다음을 통해 Amazon VPC에 대한 전체 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `AmazonVPCFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2024년 2월 8일 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
            "ec2:CreateCarrierGateway",
            "ec2:CreateCustomerGateway",
            "ec2:CreateDefaultSubnet",
            "ec2:CreateDefaultVpc",
            "ec2:CreateDhcpOptions",
            "ec2:CreateEgressOnlyInternetGateway",
            "ec2:CreateFlowLogs",
            "ec2:CreateInternetGateway",
            "ec2:CreateLocalGatewayRouteTableVpcAssociation",
            "ec2:CreateNatGateway",
            "ec2:CreateNetworkAcl",
            "ec2:CreateNetworkAclEntry",
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreateRoute",
            "ec2:CreateRouteTable",
            "ec2:CreateSecurityGroup",
            "ec2:CreateSubnet",
            "ec2:CreateTags",
            "ec2:CreateVpc",
            "ec2:CreateVpcEndpoint",
            "ec2:CreateVpcEndpointConnectionNotification",
            "ec2:CreateVpcEndpointServiceConfiguration",
            "ec2:CreateVpcPeeringConnection",
            "ec2:CreateVpnConnection",
            "ec2:CreateVpnConnectionRoute",
            "ec2:CreateVpnGateway",
            "ec2:DeleteCarrierGateway",
            "ec2:DeleteCustomerGateway",
            "ec2:DeleteDhcpOptions",
            "ec2:DeleteEgressOnlyInternetGateway",
            "ec2:DeleteFlowLogs",
            "ec2:DeleteInternetGateway",
            "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
            "ec2:DeleteNatGateway",
            "ec2:DeleteNetworkAcl",
            "ec2:DeleteNetworkAclEntry",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DeleteRoute",
            "ec2:DeleteRouteTable",
            "ec2:DeleteSecurityGroup",
            "ec2:DeleteSubnet",
            "ec2:DeleteTags",
```

```
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
```

```
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`는 AWS 관리형 정책으로, AWS Network Insights 액세스 범위 및 Network Insights 액세스 범위 분석에서 리소스를 설명하고, Network Access Analyzer를 실행하고, 태그를 생성 또는 삭제할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 15일, 22:56 UTC
- 편집된 시간: 2023년 11월 3일, 19:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonVPCReachabilityAnalyzerFullAccessPolicy

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`는 AWS 관리형 정책으로, AWS Network Insights 경로 및 Network Insights 분석에서 리소스를 설명하고, Reachability Analyzer를 실행하고, 태그를 생성 또는 삭제할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonVPCReachabilityAnalyzerFullAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 14일, 20:12 UTC
- 편집된 시간: 2023년 11월 3일, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`는 AWS 관리형 정책으로, 이 정책은 IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess 역할에 연결됩니다. 이 역할은 관리 계정을 통해 Reachability Analyzer에 대한 신뢰할 수 있는 액세스를 활성화할 때 조직의 멤버 계정에 배포됩니다. Reachability Analyzer 콘솔을 사용하여 조직 전체의 리소스를 볼 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 5월 1일, 20:38 UTC
- 편집된 시간: 2023년 5월 1일, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonVPCReadOnlyAccess

`AmazonVPCReadOnlyAccess`는 다음을 통해 Amazon VPC에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `AmazonVPCReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집 시간: 2024년 2월 8일 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AmazonWorkDocsFullAccess

`AmazonWorkDocsFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon WorkDocs에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkDocsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 16일, 23:05 UTC
- 편집된 시간: 2020년 4월 16일, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon WorkDocs에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkDocsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 1월 8일, 23:49 UTC
- 편집된 시간: 2020년 1월 8일, 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkMailEventsServiceRolePolicy

`AmazonWorkMailEventsServiceRolePolicy`는 AWS 관리형 정책으로, Amazon WorkMail Events에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 4월 16일, 16:52 UTC
- 편집된 시간: 2019년 4월 16일, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkMailFullAccess

`AmazonWorkMailFullAccess`는 AWS 관리형 정책으로, WorkMail, Directory Service, SES, EC2에 대한 전체 액세스와 KMS 메타데이터에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkMailFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 12월 21일, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkMailMessageFlowFullAccess

`AmazonWorkMailMessageFlowFullAccess`는 AWS 관리형 정책으로, WorkMail 메시지 흐름 API에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkMailMessageFlowFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 11일, 11:08 UTC
- 편집된 시간: 2021년 2월 11일, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkMailMessageFlowReadOnlyAccess

`AmazonWorkMailMessageFlowReadOnlyAccess`는 AWS 관리형 정책으로, GetRawMessageContent API의 WorkMail 메시지에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkMailMessageFlowReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 28일, 12:40 UTC
- 편집된 시간: 2021년 1월 28일, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkMailReadOnlyAccess

`AmazonWorkMailReadOnlyAccess`는 AWS 관리형 정책으로, WorkMail 및 SES에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkMailReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 7월 25일, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesAdmin

`AmazonWorkSpacesAdmin`는 AWS 관리형 정책으로, AWS SDK 및 CLI를 통해 Amazon WorkSpaces 관리 작업에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkSpacesAdmin`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 9월 22일, 22:21 UTC
- 편집된 시간: 2023년 8월 3일, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StopWorkspaces",
        "workspaces:TerminateWorkspaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess는 AWS 관리형 정책으로, Amazon WorkSpaces Application Manager에서 애플리케이션을 패키징하기 위한 관리자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesApplicationManagerAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 4월 9일, 14:03 UTC
- 편집된 시간: 2015년 4월 9일, 14:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkspacesPCAAccess

`AmazonWorkspacesPCAAccess`는 AWS 관리형 정책으로, AWS 인증서 기반 인증을 위해 사용자 AWS 계정의 Certificate Manager Private CA 리소스에 대한 전체 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkspacesPCAAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 8일, 00:25 UTC
- 편집된 시간: 2022년 11월 8일, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesSelfServiceAccess

`AmazonWorkSpacesSelfServiceAccess`는 AWS 관리형 정책으로, Workspace 셀프 서비스 작업을 수행하기 위해 Amazon WorkSpaces 백엔드 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonWorkSpacesSelfServiceAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 19:22 UTC
- 편집된 시간: 2019년 6월 27일, 19:22 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesServiceAccess

`AmazonWorkSpacesServiceAccess`는 AWS 관리형 정책으로, WorkSpace를 시작하기 위해 AWS WorkSpaces 서비스에 대한 고객 계정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesServiceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 19:19 UTC
- 편집된 시간: 2020년 3월 18일, 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly는 AWS 관리형 정책으로, AWS Management Console, SDK 및 CLI를 통해 Amazon WorkSpaces Web 및 그 종속성에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonWorkSpacesWebReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 30일, 14:20 UTC
- 편집된 시간: 2022년 11월 2일, 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy는 AWS 관리형 정책으로, Amazon WorkSpaces Web에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 30일, 13:15 UTC
- 편집된 시간: 2022년 12월 15일, 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonZocaloFullAccess

AmazonZocaloFullAccess는 AWS 관리형 정책으로, Amazon Zocalo에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AmazonZocaloFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmazonZocaloReadOnlyAccess

`AmazonZocaloReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Zocalo에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AmazonZocaloReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccess는 다음과 같은 AWS관리형 정책입니다. 개발 키트 (CDK) 를 통해 Amplify 백엔드 리소스 (Amazon AWS AppSync Cognito, Amazon S3 및 기타 관련 서비스) 를 배포할 수 있는 Amplify 전체 액세스 권한을 제공합니다. AWS 클라우드 AWS

이 정책 사용

사용자, 그룹 및 역할에 AmplifyBackendDeployFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 6일, 21:32 UTC
- 편집 시간: 2024년 1월 2일 21:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
```

```
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ]
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableSchemaResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy는 AWS 관리형 정책으로, API Gateway가 고객을 대신하여 연관된 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 17:23 UTC
- 편집된 시간: 2021년 7월 12일, 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy는 AWS 관리형 정책으로, AppIntegrations가 사용자를 대신하여 AppFlow 리소스를 관리하고 CloudWatch 지표 데이터를 게시할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 30일, 19:42 UTC
- 편집된 시간: 2022년 9월 30일, 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ApplicationAutoScalingForAmazonAppStreamAccess

`ApplicationAutoScalingForAmazonAppStreamAccess`는 AWS 관리형 정책으로, Amazon AppStream에 대한 Application Autoscaling을 활성화하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ApplicationAutoScalingForAmazonAppStreamAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 2월 6일, 21:39 UTC
- 편집된 시간: 2017년 2월 6일, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy는 AWS 관리형 정책으로, Application Discovery Service 연속 내보내기 기능에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 9일, 20:22 UTC
- 편집된 시간: 2018년 8월 13일, 22:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy는 AWS 관리형 정책으로, AWS AppRunner Networking이 사용자를 대신하여 관련 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 1월 12일, 21:02 UTC
- 편집된 시간: 2022년 1월 12일, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy는 AWS 관리형 정책으로, AWS AppRunner가 사용자를 대신하여 관련 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 14일, 19:15 UTC
- 편집된 시간: 2021년 5월 14일, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingConsoleFullAccess

`AutoScalingConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Auto Scaling에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AutoScalingConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:43 UTC
- 편집된 시간: 2018년 2월 6일, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingConsoleReadOnlyAccess

AutoScalingConsoleReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Auto Scaling에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:48 UTC
- 편집된 시간: 2017년 1월 12일, 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingFullAccess

AutoScalingFullAccess는 AWS 관리형 정책으로, Auto Scaling에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:31 UTC
- 편집된 시간: 2018년 2월 6일, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingNotificationAccessRole

AutoScalingNotificationAccessRole는 AWS 관리형 정책으로, AutoScaling Notification Access 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AutoScalingNotificationAccessRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingReadOnlyAccess

`AutoScalingReadOnlyAccess`는 AWS 관리형 정책으로, Auto Scaling에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AutoScalingReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 12일, 19:39 UTC
- 편집된 시간: 2017년 1월 12일, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AutoScalingServiceRolePolicy

`AutoScalingServiceRolePolicy`Auto Scaling에서 사용하거나 AWS 관리하는 리소스에 대한 액세스 AWS 서비스 및 리소스를 활성화하는 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 1월 8일, 23:10 UTC
- 편집 시간: 2024년 2월 29일 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWS_ConfigRole

AWS_ConfigRole AWS Config 서비스 역할에 대한 기본 정책인 AWS 관리형 정책입니다. AWS Config가 리소스 변경 사항을 추적하는 데 필요한 권한을 제공합니다. AWS

이 정책 사용

사용자, 그룹 및 역할에 AWS_ConfigRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 9월 15일, 20:30 UTC
- 편집 시간: 2024년 2월 22일 21:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

정책 버전

정책 버전: v30(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "apigateway:GET",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
```

```
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
```

```
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
```

```
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
```

```
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
```

```
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
```

```
            "datasync:DescribeLocationNfs",
            "datasync:DescribeLocationObjectStorage",
            "datasync:DescribeLocationS3",
            "datasync:DescribeLocationSmb",
            "datasync:DescribeTask",
            "datasync:ListAgents",
            "datasync:ListLocations",
            "datasync:ListTagsForResource",
            "datasync:ListTasks",
            "dax:DescribeClusters",
            "dax:DescribeParameterGroups",
            "dax:DescribeParameters",
            "dax:DescribeSubnetGroups",
            "dax:ListTags",
            "detective:ListGraphs",
            "detective:ListTagsForResource",
            "devicefarm:GetInstanceProfile",
            "devicefarm:GetNetworkProfile",
            "devicefarm:GetProject",
            "devicefarm:GetTestGridProject",
            "devicefarm:ListInstanceProfiles",
            "devicefarm:ListNetworkProfiles",
            "devicefarm:ListProjects",
            "devicefarm:ListTagsForResource",
            "devicefarm:ListTestGridProjects",
            "devops-guru:GetResourceCollection",
            "dms:DescribeCertificates",
            "dms:DescribeEndpoints",
            "dms:DescribeEventSubscriptions",
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationSubnetGroups",
            "dms:DescribeReplicationTaskAssessmentRuns",
            "dms:DescribeReplicationTasks",
            "dms:ListTagsForResource",
            "ds:DescribeDirectories",
            "ds:DescribeDomainControllers",
            "ds:DescribeEventTopics",
            "ds:ListLogSubscriptions",
            "ds:ListTagsForResource",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeTable",
```

```
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
```

```
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
```

```
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
```

```
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
```

```
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
```

```
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
```

```
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
```

```
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
```

```
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
```

```
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
```

```
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
```

```
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
```

```
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
```

```
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
```

```
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
```

```
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
```

```
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
```

```
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
```

```
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
```

```
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
```

```
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSAccountActivityAccess

AWSAccountActivityAccess는 AWS 관리형 정책으로, 사용자가 계정 활동 페이지에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAccountActivityAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2023년 3월 7일, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAccountManagementFullAccess

`AWSAccountManagementFullAccess`는 AWS 관리형 정책으로, AWS Account Management에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAccountManagementFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 30일, 23:20 UTC
- 편집된 시간: 2021년 9월 30일, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAccountManagementReadOnlyAccess

`AWSAccountManagementReadOnlyAccess`는 AWS 관리형 정책으로, AWS Account Management에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAccountManagementReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 9월 30일, 23:29 UTC
- 편집된 시간: 2021년 9월 30일, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAccountUsageReportAccess

AWSAccountUsageReportAccess는 AWS 관리형 정책으로, 사용자가 계정 사용 보고서 페이지에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAccountUsageReportAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAgentlessDiscoveryService

`AWSAgentlessDiscoveryService`는 AWS 관리형 정책으로, Discovery Agentless Connector가 AWS Application Discovery Service에 등록할 수 있도록 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAgentlessDiscoveryService`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 8월 2일, 01:35 UTC
- 편집된 시간: 2020년 2월 24일, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppFabricFullAccess

`AWSAppFabricFullAccess`는 AWS 관리형 정책으로, AWS AppFabric 서비스에 대한 전체 액세스와 S3, Kinesis, KMS와 같은 종속 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAppFabricFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 19:51 UTC
- 편집된 시간: 2023년 6월 27일, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppFabricReadOnlyAccess

`AWSAppFabricReadOnlyAccess`는 AWS 관리형 정책으로, AWS AppFabric에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSAppFabricReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 19:52 UTC
- 편집된 시간: 2023년 6월 27일, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy는 AWS 관리형 정책으로, AppFabric가 사용자를 대신하여 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 26일, 21:07 UTC
- 편집된 시간: 2023년 6월 26일, 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy는 AWS 관리형 정책으로, AppStream 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 19:04 UTC
- 편집된 시간: 2017년 10월 20일, 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy는 AWS 관리형 정책으로, Cassandra 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 3월 18일, 22:49 UTC
- 편집된 시간: 2020년 3월 18일, 22:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingComprehendEndpointPolicy

`AWSApplicationAutoscalingComprehendEndpointPolicy`는 AWS 관리형 정책으로, Comprehend 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 14일, 18:39 UTC
- 편집된 시간: 2019년 11월 14일, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy는 AWS 관리형 정책으로, 사용자 지정 리소스 조정을 위해 APIGateway 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 4일, 23:22 UTC
- 편집된 시간: 2018년 6월 4일, 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy는 AWS 관리형 정책으로, DynamoDB 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 20일, 21:34 UTC
- 편집된 시간: 2017년 10월 20일, 21:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`는 AWS 관리형 정책으로, EC2 Spot Fleet 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 25일, 18:23 UTC
- 편집된 시간: 2017년 10월 25일, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy는 AWS 관리형 정책으로, EC2 Container Service 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 25일, 23:53 UTC
- 편집된 시간: 2017년 10월 25일, 23:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy는 AWS 관리형 정책으로, Amazon ElastiCache 및 Amazon CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 17일, 23:41 UTC
- 편집된 시간: 2021년 8월 17일, 23:41 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingEMRInstanceGroupPolicy

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`는 AWS 관리형 정책으로, Elastic Map Reduce 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 26일, 00:57 UTC
- 편집된 시간: 2017년 10월 26일, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy는 AWS 관리형 정책으로, Managed Streaming for Apache Kafka 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 24일, 18:36 UTC
- 편집된 시간: 2020년 8월 24일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy는 AWS 관리형 정책으로, Lambda 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 21일, 20:04 UTC
- 편집된 시간: 2019년 10월 21일, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy는 AWS 관리형 정책으로, Amazon Neptune 및 Amazon CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 2일, 21:14 UTC
- 편집된 시간: 2021년 9월 2일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy는 AWS 관리형 정책으로, RDS 및 CloudWatch에 액세스할 수 있도록 Application Auto Scaling에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2017년 10월 17일, 17:46 UTC
- 편집된 시간: 2018년 8월 7일, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationAutoscalingSageMakerEndpointPolicy

`AWSApplicationAutoscalingSageMakerEndpointPolicy`Application Auto Scaling에 SageMaker 및 CloudWatch 에 대한 액세스 권한을 부여하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 2월 6일, 19:58 UTC
- 편집된 시간: 2023년 11월 13일, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess는 AWS 관리형 정책으로, Discovery Agent가 AWS Application Discovery Service에 등록할 수 있도록 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationDiscoveryAgentAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 5월 11일, 21:38 UTC
- 편집된 시간: 2020년 2월 24일, 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationDiscoveryAgentlessCollectorAccess

`AWSApplicationDiscoveryAgentlessCollectorAccess`는 AWS 관리형 정책으로, Application Discovery Service Agentless Collector가 Application Discovery Service와 자동으로 업데이트, 등록 및 통신할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationDiscoveryAgentlessCollectorAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 21:00 UTC
- 편집된 시간: 2022년 8월 16일, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess는 AWS 관리형 정책으로, AWS Application Discovery Service에서 유지 관리하는 구성 항목을 보고 태그를 지정할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationDiscoveryServiceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 5월 11일, 21:30 UTC
- 편집된 시간: 2019년 6월 19일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationAgentInstallationPolicy

`AWSApplicationMigrationAgentInstallationPolicy`는 AWS 관리형 정책으로, 이 정책은 AWS 외부 서버를 AWS로 마이그레이션하기 위해 Application Migration Service(MGN)와 함께 사용되는 AWS Replication Agent를 설치할 수 있도록 허용합니다. 이 정책을 AWS Replication Agent를 설치할 때 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationAgentInstallationPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 6월 19일, 07:51 UTC
- 편집된 시간: 2022년 9월 20일, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationAgentPolicy

`AWSApplicationMigrationAgentPolicy`는 AWS 관리형 정책으로, 이 정책은 외부 서버를 AWS로 마이그레이션하기 위해 AWS Application Migration Service(MGN)와 함께 사용되는 AWS Replication Agent를 설치 및 사용할 수 있도록 허용합니다. 이 정책을 AWS Replication Agent를 설치할 때 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationAgentPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 07:00 UTC
- 편집된 시간: 2022년 9월 20일, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationAgentPolicy_v2

AWSApplicationMigrationAgentPolicy_v2는 AWS 관리형 정책으로, 이 정책은 외부 서버를 AWS로 마이그레이션하기 위해 AWS Application Migration Service(MGN)와 함께 사용되는 AWS Replication Agent를 사용할 수 있도록 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationAgentPolicy_v2를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 6월 6일, 14:14 UTC
- 편집된 시간: 2022년 6월 6일, 14:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationConversionServerPolicy

`AWSApplicationMigrationConversionServerPolicy`는 AWS 관리형 정책으로, 이 정책은 Application Migration Service에서 시작하는 EC2 인스턴스인 Application Migration Service(MGN) Conversion Server가 MGN 서비스와 통신할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery에 의해 (EC2 Instance Profile로) MGN Conversion Servers에 연결되며, 필요할 때 MGN에 의해 자동으로 시작 및 종료됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다. MGN Conversion Servers는 사용자가 MGN 콘솔, CLI 또는 API를 사용하여 테스트 또는 컷오버 인스턴스를 시작하도록 선택할 때 Application Migration Service에서 사용됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationConversionServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 06:48 UTC
- 편집된 시간: 2021년 4월 7일, 06:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access는 AWS 관리형 정책으로, 이 정책은 애플리케이션 Application Migration Service(MGN)를 사용하여 마이그레이션된 서버를 EC2 인스턴스로 시작하는 데 필요한 Amazon EC2 작업을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationEC2Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 07:05 UTC
- 편집된 시간: 2023년 2월 6일, 16:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationFullAccess

`AWSApplicationMigrationFullAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Application Migration Service(MGN)의 모든 퍼블릭 API에 대한 권한과 KMS 키 정보를 읽을 수 있는 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 06:56 UTC
- 편집된 시간: 2023년 4월 20일, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationMGHAccess

`AWSApplicationMigrationMGHAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Application Migration Service(MGN)가 MGN을 사용하여 AWS Migration Hub(MGH)로 마이그레이션되는 서버의 진행 상황에 대한 메타 데이터를 보낼 수 잇도록 허용합니다. MGN은 이 정책이 연결된 IAM 역할을 자동으로 생성하고 이 역할을 맡습니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationMGHAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 07:10 UTC
- 편집된 시간: 2021년 4월 7일, 07:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationReadOnlyAccess

`AWSApplicationMigrationReadOnlyAccess`는 AWS 관리형 정책으로, 이 정책은 Application Migration Service(MGN) 의 모든 읽기 전용 퍼블릭 API와 MGN 콘솔을 완전히 읽기 전용으로 사용하는 데 필요한 기타 AWS 서비스의 일부 읽기 전용 API에 대한 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 7일, 07:15 UTC
- 편집된 시간: 2023년 3월 20일, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationReplicationServerPolicy

`AWSApplicationMigrationReplicationServerPolicy`는 AWS 관리형 정책으로, 이 정책은 Application Migration Service에서 시작하는 EC2 인스턴스인 Application Migration Service(MGN) Replication Servers가 MGN 서비스와 통신하고 사용자 AWS 계정에 EBS 스냅샷을 생성할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 Application Migration Service에 의해 (EC2 Instance Profile로) MGN Replication Servers에 연결되며, 필요에 따라 MGN에 의해 자동으로 시작 및 종료됩니다. MGN Replication Servers는 MGN을 사용하여 관리되는 마이그레이션 프로세스의 일환으로 외부 서버에서 AWS로의 데이터 복제를 용이하게 하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSApplicationMigrationReplicationServerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 4월 7일, 07:21 UTC
- 편집된 시간: 2021년 4월 7일, 07:21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy는 AWS 관리형 정책으로, 이 정책은 AWS Application Migration Service(AWS MGN)이 EC2(교차 리전 및 교차 AZ)에서 실행되는 소스 서버를 마이그레이션하기 위해 사용되는 AWS Replication Agent를 설치 및 사용할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 EC2 Instance에 (EC2 Instance Profile로) 연결되어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationServiceEc2InstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 22일, 13:19 UTC
- 편집 시간: 2024년 1월 3일 14:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy는 AWS 관리형 정책으로, AWS Application Migration Service가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 7일, 06:43 UTC
- 편집된 시간: 2023년 6월 20일, 09:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess는 AWS 관리형 정책으로, 이 정책은 Application Migration Service(MGN)를 사용하여 사용자 지정 마이그레이션 후 명령 SSM 문서를 실행하는 데 필요한 Amazon SSM 작업에 대한 액세스를 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationSSMAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 09:29 UTC
- 편집된 시간: 2023년 3월 20일, 10:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicy는 AWS 관리형 정책으로, 이 정책은 AWS 외부 서버를 AWS로 마이그레이션하기 위해 Application Migration Service(MGN)와 함께 사용되는 AWS VCenter Client를 설치 및 사용할 수 있도록 허용합니다. 이 정책을 AWS VCenter Client를 설치할 때 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSApplicationMigrationVCenterClientPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 8일, 12:53 UTC
- 편집된 시간: 2021년 11월 8일, 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess는 AWS 관리형 정책으로, 가상 노드 구성에 액세스하기 위한 App Mesh Envoy 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshEnvoyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 3일, 21:29 UTC
- 편집된 시간: 2019년 7월 3일, 21:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshFullAccess

AWSAppMeshFullAccess는 AWS 관리형 정책으로, AWS App Mesh API 및 관리 콘솔에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 16일, 17:50 UTC
- 편집된 시간: 2021년 1월 7일, 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess는 AWS 관리형 정책으로, 가상 노드 구성에 액세스하기 위한 App Mesh Preview Envoy 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshPreviewEnvoyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 8월 5일, 23:32 UTC
- 편집된 시간: 2019년 8월 5일, 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshPreviewServiceRolePolicy

`AWSAppMeshPreviewServiceRolePolicy`는 AWS 관리형 정책으로, AWS App Mesh에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 19일, 19:07 UTC
- 편집된 시간: 2019년 8월 21일, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshReadOnly

AWSAppMeshReadOnly는 AWS 관리형 정책으로, AWS App Mesh API 및 관리 콘솔에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppMeshReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 16일, 17:51 UTC
- 편집된 시간: 2021년 1월 7일, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy는 AWS 관리형 정책으로, AWS AppMesh에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 3일, 18:30 UTC
- 편집된 시간: 2023년 10월 10일, 16:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppRunnerFullAccess

AWSAppRunnerFullAccess는 AWS 관리형 정책으로, 모든 App Runner 작업에 대한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppRunnerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 1월 11일, 04:02 UTC
- 편집된 시간: 2022년 1월 11일, 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppRunnerReadOnlyAccess

AWSAppRunnerReadOnlyAccess는 AWS 관리형 정책으로, App Runner 리소스에 대한 세부 정보를 나열하고 볼 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppRunnerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 24일, 21:24 UTC
- 편집된 시간: 2022년 2월 24일, 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppRunnerServicePolicyForECRAccess

AWSAppRunnerServicePolicyForECRAccess는 AWS 관리형 정책으로, 고객 계정의 Amazon ECR 리소스에 대한 읽기 권한을 부여하는 AWS App Runner 서비스 정책입니다. App Runner 서비스를 생성하거나 업데이트할 때 App Runner에 전달되는 역할에 사용하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppRunnerServicePolicyForECRAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 5월 14일, 19:17 UTC
- 편집된 시간: 2021년 5월 14일, 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppSyncAdministrator

AWSAppSyncAdministrator는 AWS 관리형 정책으로, 콘솔을 통해 액세스하기에는 충분하지 않지만 AppSync 서비스에 대한 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:20 UTC
- 편집된 시간: 2019년 11월 4일, 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess는 AWS 관리형 정책으로, 콘솔을 통해 또는 독립적으로 AppSync 서비스에 대한 전체 호출 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncInvokeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:21 UTC
- 편집된 시간: 2018년 3월 20일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppSyncPushToCloudWatchLogs

`AWSAppSyncPushToCloudWatchLogs`는 AWS 관리형 정책으로, AppSync가 사용자의 CloudWatch 계정에 로그를 푸시할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncPushToCloudWatchLogs를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 4월 9일, 19:38 UTC
- 편집된 시간: 2018년 4월 9일, 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor는 AWS 관리형 정책으로, 스키마를 생성, 업데이트 및 쿼리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAppSyncSchemaAuthor를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 20일, 21:21 UTC
- 편집된 시간: 2023년 2월 1일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicy는 AWS 관리형 정책으로, AppSync에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 1월 21일, 19:56 UTC
- 편집된 시간: 2020년 1월 21일, 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSArtifactAccountSync

AWSArtifactAccountSync는 AWS 관리형 정책으로, AWS Organizations의 작업에 대한 AWS Artifact 읽기 전용 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSArtifactAccountSync를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 4월 10일, 23:04 UTC
- 편집된 시간: 2018년 4월 10일, 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSArtifactReportsReadOnlyAccess

`AWSArtifactReportsReadOnlyAccess`AWSArtifact 서비스 보고서에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSArtifactReportsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2024년 1월 2일 22:42 UTC
- 편집 시간: 2024년 1월 2일 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSArtifactServiceRolePolicy

`AWSArtifactServiceRolePolicy`는 AWS 관리형 정책으로, AWS Artifact가 AWS Organizations 서비스를 통해 조직에 대한 정보를 수집할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 8월 21일, 20:27 UTC
- 편집된 시간: 2023년 8월 21일, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess는 AWS 관리형 정책으로, AWS Audit Manager를 활성화 또는 비활성화하고, 설정을 업데이트하고, 평가, 제어 및 프레임워크를 관리할 수 있는 관리 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSAuditManagerAdministratorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 11일, 20:02 UTC
- 편집된 시간: 2022년 4월 30일, 00:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAuditManagerServiceRolePolicy

`AWSAuditManagerServiceRolePolicy`는 AWS 관리형 정책으로, AWS Audit Manager에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 8일, 15:12 UTC
- 편집 시간: 2023년 12월 6일 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
```

```
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
```

```
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDbClusterEndpoints",
        "rds:DescribeDbClusterParameterGroups",
        "rds:DescribeDbClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDbSecurityGroups",
        "redshift:DescribeClusters",
        "route53:GetQueryLoggingConfig",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "securityhub:DescribeStandards",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf:ListActivatedRulesInRuleGroup"
      ],
      "Resource" : "*",
      "Sid" : "AuditManagerAPICallAccess"
    },
    {
      "Sid" : "AuditManagerS3GetBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy는 AWS 관리형 정책으로, AWS Auto Scaling에 규모 조정 계획의 Auto Scaling 그룹에 대해 정기적으로 용량을 예측하고 예약된 규모 조정 작업을 생성할 수 있는 권한을 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 23일, 22:46 UTC
- 편집된 시간: 2018년 8월 23일, 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
```

```
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupAuditAccess

AWSBackupAuditAccess는 AWS 관리형 정책으로, 이 정책은 사용자에게 AWS Backup 리소스 및 활동에 대한 기대치를 정의하는 제어 및 프레임워크를 생성하고, 정의된 제어 및 프레임워크에 따라 AWS Backup 리소스 및 활동을 감사할 수 있는 권한을 부여합니다. 이 정책은 AWS Config 및 유사한 서비스에 감사 수행에 대한 사용자 기대치를 설명할 수 있는 권한을 부여합니다. 또한 이 정책은 S3 및 유사한 서비스에 감사 보고서를 전송할 수 있는 권한을 부여하고 사용자가 감사 보고서를 검색하고 열람할 수 있도록 합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupAuditAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 8월 24일, 01:02 UTC
- 편집된 시간: 2023년 4월 10일, 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupAuditAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupDataTransferAccess

`AWSBackupDataTransferAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Backint 에이전트가 AWS Backup Storage 플레인을 사용하여 백업 데이터 전송을 완료할 수 있도록 허용합니다. 이 역할을 Backint 에이전트와 함께 SAP HANA를 실행하는 Amazon EC2 Instances가 맡은 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBackupDataTransferAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 22:48 UTC
- 편집된 시간: 2022년 11월 10일, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupFullAccess

AWSBackupFullAccess는 AWS 관리형 정책으로, 이 정책은 백업 관리자를 위한 것으로, 백업 계획 생성 또는 편집, 백업 계획에 AWS 리소스 할당, 백업 삭제, 백업 복원을 포함한 AWS Backup 작업에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 18일, 22:21 UTC
- 편집 시간: 2023년 11월 27일 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
```

```
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
```

```
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
```

```
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
```

```
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
```

```
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`는 AWS 관리형 정책으로, 사용자를 대신하여 Virtual Machines의 메타데이터를 동기화할 수 있는 AWS BackupGateway 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 12월 15일, 19:43 UTC

- 편집된 시간: 2022년 12월 15일, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupOperatorAccess

AWSBackupOperatorAccess는 AWS 관리형 정책으로, 이 정책은 사용자에게 백업 계획에 AWS 리소스를 할당하고, 온디맨드 백업을 생성하고, 백업을 복원할 수 있는 권한을 부여합니다. 이 정책은 사용자가 백업 계획을 생성 또는 편집하도록 허용하거나 예약된 백업을 생성한 후 삭제하도록 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupOperatorAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 18일, 22:23 UTC
- 편집된 시간: 2023년 9월 6일, 20:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
```

```
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupOrganizationAdminAccess

`AWSBackupOrganizationAdminAccess`는 AWS 관리형 정책으로, 이 정책은 교차 계정 백업 관리를 사용하여 조직의 백업을 관리하는 백업 관리자를 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBackupOrganizationAdminAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 24일, 16:23 UTC
- 편집된 시간: 2022년 11월 18일, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA는 AWS 관리형 정책으로, Amazon EC2에서 SAP HANA의 백업을 복원할 수 있는 AWS Backup 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupRestoreAccessForSAPHANA를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 10일, 22:43 UTC
- 편집된 시간: 2022년 11월 10일, 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceLinkedRolePolicyForBackup

`AWSBackupServiceLinkedRolePolicyForBackup`는 AWS 관리형 정책으로, 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 AWS Backup 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 2일, 23:08 UTC
- 편집 시간: 2023년 12월 15일 22:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
```

```
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
```

```
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
```

```
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
```

```
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceLinkedRolePolicyForBackupTest

`AWSBackupServiceLinkedRolePolicyForBackupTest`는 AWS 관리형 정책으로, 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 AWS Backup 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2020년 5월 12일, 17:37 UTC
- 편집된 시간: 2020년 5월 12일, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceRolePolicyForBackup

AWSBackupServiceRolePolicyForBackup는 AWS 관리형 정책으로, 여러 AWS 서비스에서 사용자를 대신하여 백업을 생성할 수 있는 AWS Backup 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForBackup를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 1월 10일, 21:01 UTC
- 편집 시간: 2023년 12월 15일 22:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup

정책 버전

정책 버전: v18(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
```

```
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
```

```
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
```

```
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
```

```
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
```

```
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
```

```
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceRolePolicyForRestores

`AWSBackupServiceRolePolicyForRestores`는 AWS 관리형 정책으로, 여러 AWS 서비스에서 사용자를 대신하여 복원을 수행할 수 있는 AWS Backup 권한을 제공합니다. 이 정책에는 복원 프로세스의 일부인 EBS 볼륨, RDS 인스턴스, EFS 파일 시스템과 같은 AWS 리소스를 생성하고 삭제할 수 있는 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBackupServiceRolePolicyForRestores`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2019년 1월 12일, 00:23 UTC
- 편집 시간: 2023년 12월 15일 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

정책 버전

정책 버전: v20(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
```

```
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
```

```
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
```

```
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup는 AWS 관리형 정책으로, AWS Backup이 모든 S3 버킷의 데이터를 백업하는 데 필요한 권한이 포함되어 있는 정책입니다. 여기에는 모든 S3 객체에 대한 읽기 액세스와 모든 KMS 키에 대한 암호 해독 액세스가 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForS3Backup를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 18일, 17:40 UTC
- 편집된 시간: 2022년 9월 1일, 16:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore AWS 관리형 정책으로, Backup이 S3 AWS 백업을 버킷에 복원하는 데 필요한 권한이 포함되어 있는 정책입니다. 여기에는 모든 S3 버킷에 대한 읽기/쓰기 권한과 모든 KMS 키에 대한 GenerateKey 및 DescribeKey에 대한 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBackupServiceRolePolicyForS3Restore를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 2월 18일, 17:39 UTC
- 편집된 시간: 2023년 2월 7일, 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBatchFullAccess

`AWSBatchFullAccess`는 AWS 관리형 정책으로, AWS Batch 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBatchFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 6일, 19:35 UTC
- 편집된 시간: 2022년 10월 24일, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBatchServiceEventTargetRole

`AWSBatchServiceEventTargetRole`는 AWS 관리형 정책으로, AWS Batch Job Submission을 위해 CloudWatch Event Target을 활성화하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBatchServiceEventTargetRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 2월 28일, 22:31 UTC
- 편집된 시간: 2018년 2월 28일, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBatchServiceRole

`AWSBatchServiceRole`는 AWS 관리형 정책으로, EC2, Autoscaling, EC2 Container 서비스 및 Cloudwatch Logs를 포함한 관련 서비스에 대한 액세스를 허용하는 AWS Batch 서비스 역할 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBatchServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 6일, 19:36 UTC
- 편집 시간: 2023년 12월 5일 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBillingConductorFullAccess

AWSBillingConductorFullAccess는 AWS 관리형 정책으로, AWSBillingConductorFullAccess 관리형 정책을 사용하여 AWS Billing Conductor(ABC) 콘솔 및 API에 대한 완전한 액세스를 허용합니다. 이 정책을 통해 사용자는 ABC 리소스를 나열, 생성 및 삭제할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingConductorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 13일, 18:02 UTC
- 편집된 시간: 2022년 4월 13일, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBillingConductorReadOnlyAccess

AWSBillingConductorReadOnlyAccess는 AWS 관리형 정책으로, AWSBillingConductorReadOnlyAccess 관리형 정책을 사용하여 AWS Billing Conductor(ABC) 콘솔 및 API에 대한 읽기 전용 액세스를 허용합니다. 이 정책은 모든 ABC 리소스를 보고 나열할 수 있는 권한을 부여합니다. 리소스를 생성 또는 삭제하는 기능은 포함되지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingConductorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 13일, 18:02 UTC
- 편집된 시간: 2022년 4월 13일, 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "organizations:ListAccounts",
        "pricing:DescribeServices"
      ],
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess는 AWS 관리형 정책으로, 사용자가 결제 콘솔에서 청구서를 볼 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBillingReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 27일, 20:08 UTC
- 편집 시간: 2024년 1월 17일 18:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
```

```
        "payments:ListPaymentPreferences",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`는 AWS 관리형 정책으로, 이 정책은 AWS 리소스를 제어할 수 있는 권한을 부여합니다. 예를 들어 AWS Systems Manager(SSM) 스크립트를 실행하여 EC2 또는 RDS를 시작 및 중지합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 5월 25일, 19:03 UTC
- 편집된 시간: 2022년 5월 25일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBudgetsActionsWithAWSResourceControlAccess

`AWSBudgetsActionsWithAWSResourceControlAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 실행 중인 AWS 리소스의 상태를 제어하기 위해 Budgets Actions을 사용하는 것을 포함하여 AWS Budgets Actions에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBudgetsActionsWithAWSResourceControlAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 15일, 17:19 UTC
- 편집된 시간: 2020년 10월 15일, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBudgetsReadOnlyAccess

`AWSBudgetsReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Budgets Console에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSBudgetsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 15일, 17:18 UTC
- 편집된 시간: 2020년 10월 15일, 17:18 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBugBustFullAccess

`AWSBugBustFullAccess`는 AWS 관리형 정책으로, 사용자에게 AWS BugBust 콘솔에 대한 전체 액세스를 부여하는 IAM 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBugBustFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 6월 24일, 07:03 UTC
- 편집된 시간: 2021년 7월 22일, 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBugBustPlayerAccess

AWSBugBustPlayerAccess는 AWS 관리형 정책으로, 사용자에게 AWS BugBust 이벤트에 참여할 수 있는 액세스를 부여하는 IAM 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSBugBustPlayerAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 6월 24일, 07:15 UTC
- 편집된 시간: 2021년 6월 24일, 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy는 AWS 관리형 정책으로, AWS BugBust에 사용자를 대신하여 리소스에 액세스할 수 있도록 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 24일, 06:59 UTC
- 편집된 시간: 2021년 6월 24일, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess는 AWS 관리형 정책으로, AWS Certificate Manager(ACM)에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 21일, 17:02 UTC
- 편집된 시간: 2020년 8월 17일, 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerPrivateCAAuditor

`AWSCertificateManagerPrivateCAAuditor`는 AWS 관리형 정책으로, AWS Certificate Manager Private Certificate Authority에 대한 감사자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCertificateManagerPrivateCAAuditor`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:51 UTC
- 편집된 시간: 2020년 8월 17일, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerPrivateCAFullAccess

`AWSCertificateManagerPrivateCAFullAccess`는 AWS 관리형 정책으로, AWS Certificate Manager Private Certificate Authority에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCertificateManagerPrivateCAFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:54 UTC
- 편집된 시간: 2018년 10월 23일, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerPrivateCAPrivilegedUser

`AWSCertificateManagerPrivateCAPrivilegedUser`는 AWS 관리형 정책으로, AWS Certificate Manager Private Certificate Authority에 대한 권한 있는 인증서 사용자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCertificateManagerPrivateCAPrivilegedUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 20일, 17:43 UTC
- 편집된 시간: 2019년 6월 20일, 17:43 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerPrivateCAReadOnly

`AWSCertificateManagerPrivateCAReadOnly`는 AWS 관리형 정책으로, AWS Certificate Manager Private Certificate Authority에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCertificateManagerPrivateCAReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 10월 23일, 16:57 UTC
- 편집된 시간: 2020년 8월 17일, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerPrivateCAUser

AWSCertificateManagerPrivateCAUser는 AWS 관리형 정책으로, AWS Certificate Manager Private Certificate Authority에 대한 인증서 사용자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerPrivateCAUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 23일, 16:53 UTC
- 편집된 시간: 2019년 6월 20일, 17:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCertificateManagerReadOnly

AWSCertificateManagerReadOnly는 AWS 관리형 정책으로, AWS Certificate Manager(ACM)에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCertificateManagerReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 21일, 17:07 UTC
- 편집된 시간: 2021년 3월 15일, 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
```

```
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSChatbotServiceLinkedRolePolicy

`AWSChatbotServiceLinkedRolePolicy`는 AWS 관리형 정책으로, AWS Chatbot에서 사용하는 서비스 연결 역할인 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 18일, 16:39 UTC
- 편집된 시간: 2019년 11월 18일, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCleanRoomsFullAccess

`AWSCleanRoomsFullAccess` AWS Clean Rooms 리소스에 대한 전체 액세스 및 관련 리소스에 대한 액세스를 허용하는 AWS 관리형 AWS 서비스정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:10 UTC
- 편집 시간: 2024년 3월 21일 오후 5시 35분 (UTC)
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSCleanRoomsFullAccessNoQuerying

AWSCleanRoomsFullAccessNoQuerying는 AWS 관리형 정책으로, 공동 작업 쿼리를 제외한 AWS Clean Rooms 리소스에 대한 전체 액세스와 관련 AWS 서비스에 대한 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsFullAccessNoQuerying를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:12 UTC
- 편집된 시간: 2023년 7월 31일, 20:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:CreateAnalysisTemplate",
```

```
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCleanRoomsMLFullAccess

`AWSCleanRoomsMLFullAccess`AWSClean Rooms ML 리소스에 대한 전체 액세스 및 관련 리소스에 대한 액세스를 허용하는 AWS관리형 AWS 서비스 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCleanRoomsMLFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 29일, 21:02 UTC
- 편집 시간: 2023년 11월 29일, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
```

```
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
```

```
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccessAWSClean Rooms ML 리소스에 대한 읽기 전용 액세스와 관련 AWS 클린 룸 리소스에 대한 읽기 전용 액세스를 허용하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsMLReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 29일 20:55 UTC
- 편집 시간: 2023년 11월 29일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCleanRoomsReadOnlyAccess

AWSCleanRoomsReadOnlyAccess는 AWS 관리형 정책으로, AWS Clean Rooms 리소스에 대한 읽기 전용 액세스와 관련 AWS Glue 및 Amazon CloudWatch Logs 리소스에 대한 읽기 전용 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCleanRoomsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 12일, 16:10 UTC
- 편집된 시간: 2023년 1월 12일, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloud9Administrator

`AWSCloud9Administrator`는 AWS 관리형 정책으로, AWS Cloud9에 대한 관리자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloud9Administrator`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:17 UTC
- 편집된 시간: 2023년 10월 11일, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloud9EnvironmentMember

AWSCloud9EnvironmentMember는 AWS 관리형 정책으로, AWS Cloud9 공유 개발 환경에 초대될 수 있는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloud9EnvironmentMember를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:18 UTC
- 편집된 시간: 2023년 10월 11일, 12:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloud9ServiceRolePolicy

`AWSCloud9ServiceRolePolicy`는 AWS 관리형 정책으로, AWS Cloud9에 대한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 30일, 13:44 UTC
- 편집된 시간: 2022년 1월 17일, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloud9SSMInstanceProfile

`AWSCloud9SSMInstanceProfile`는 AWS 관리형 정책으로, 이 정책은 Cloud9이 SSM Session Manager를 사용하여 인스턴스에 연결할 수 있도록 하는 InstanceProfile의 역할을 연결하는 데 사용됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloud9SSMInstanceProfile`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 14일, 11:40 UTC
- 편집된 시간: 2020년 5월 14일, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloud9User

`AWSCloud9User`는 AWS 관리형 정책으로, AWS Cloud9 개발 환경을 생성하고 소유한 환경을 관리할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloud9User`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 30일, 16:16 UTC
- 편집된 시간: 2023년 10월 11일, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudFormationFullAccess

AWSCloudFormationFullAccess는 AWS 관리형 정책으로, AWS CloudFormation에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudFormationFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 26일, 21:50 UTC
- 편집된 시간: 2019년 7월 26일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudFormationReadOnlyAccess

`AWSCloudFormationReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CloudFormation에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudFormationReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2019년 11월 13일, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudFrontLogger

`AWSCloudFrontLogger`는 AWS 관리형 정책으로, CloudFront Logger에 CloudWatch Logs에 대한 쓰기 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 6월 12일, 20:15 UTC
- 편집된 시간: 2019년 11월 22일, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudHSMFullAccess

`AWSCloudHSMFullAccess`는 AWS 관리형 정책으로, 모든 CloudHSM 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudHSMFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudHSMReadOnlyAccess

AWSCloudHSMReadOnlyAccess는 AWS 관리형 정책으로, 모든 CloudHSM 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudHSMReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudHSMRole

AWSCloudHSMRole은 AWS 관리형 정책으로, AWS CloudHSM 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudHSMRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudMapDiscoverInstanceAccess

`AWSCloudMapDiscoverInstanceAccess`는 AWS 관리형 정책으로, AWS 클라우드 Map discovery API에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudMapDiscoverInstanceAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 00:02 UTC

- 편집된 시간: 2023년 9월 20일, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudMapFullAccess

AWSCloudMapFullAccess는 AWS 관리형 정책으로, 모든 AWS 클라우드 Map 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 23:57 UTC
- 편집된 시간: 2020년 7월 29일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudMapReadOnlyAccess

`AWSCloudMapReadOnlyAccess`는 AWS 관리형 정책으로, 모든 AWS 클라우드 Map 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudMapReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 23:45 UTC
- 편집된 시간: 2023년 9월 20일, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudMapRegisterInstanceAccess

`AWSCloudMapRegisterInstanceAccess`는 AWS 관리형 정책으로, AWS 클라우드 Map 작업에 대한 등록자 수준 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudMapRegisterInstanceAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 00:04 UTC
- 편집된 시간: 2023년 9월 20일, 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudShellFullAccess

`AWSCloudShellFullAccess`는 AWS 관리형 정책으로, 모든 기능과 함께 AWS CloudShell을 사용하여 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudShellFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 18:07 UTC
- 편집된 시간: 2020년 12월 15일, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudTrail_FullAccess

`AWSCloudTrail_FullAccess`는 AWS 관리형 정책으로, AWS CloudTrail에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCloudTrail_FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 8일, 23:41 UTC

- 편집된 시간: 2021년 2월 22일, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudTrail_ReadOnlyAccess

AWSCloudTrail_ReadOnlyAccess는 AWS 관리형 정책으로, AWS CloudTrail에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCloudTrail_ReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 6월 14일, 17:19 UTC
- 편집된 시간: 2022년 6월 14일, 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents라는 이름이 지정된 서비스 연결 역할에서 사용됩니다. CloudWatch는 CloudWatch 경보가 ALARM 상태가 될 때 이 서비스 연결 역할을 사용하여 AWS System Manager Incident Manager 작업을 수행합니다. 이 정책은 사용자를 대신하여 인시던트를 시작할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 27일, 13:30 UTC
- 편집된 시간: 2021년 4월 27일, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeArtifactAdminAccess

`AWSCodeArtifactAdminAccess`는 AWS 관리형 정책으로, AWS Management Console를 통해 AWS CodeArtifact에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeArtifactAdminAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 16일, 23:53 UTC
- 편집된 시간: 2020년 6월 16일, 23:53 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeArtifactReadOnlyAccess

AWSCodeArtifactReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CodeArtifact에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeArtifactReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 25일, 21:23 UTC
- 편집된 시간: 2020년 6월 25일, 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess는 AWS 관리형 정책으로, AWS Management Console를 통해 AWS CodeBuild에 대한 전체 액세스를 제공합니다. 또한 AmazonS3ReadOnlyAccess를 연결하여 빌드 아티팩트를 다운로드할 수 있는 액세스를 제공하고, IAMFullAccess를 연결하여 CodeBuild에 대한 서비스 역할을 생성하고 관리합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:04 UTC
- 편집된 시간: 2023년 7월 31일, 23:06 UTC

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

정책 버전

정책 버전: v13(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
```

```
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
```

```
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
```

```
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CodeBuild에 대한 액세스를 제공하지만 CodeBuild 프로젝트 관리는 허용하지 않습니다. 또한 AmazonS3ReadOnlyAccess를 연결하여 빌드 아티팩트 다운로드에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildDeveloperAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:02 UTC
- 편집된 시간: 2023년 7월 31일, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
```

```
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeBuildReadOnlyAccess

AWSCodeBuildReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CodeBuild에 대한 읽기 전용 액세스를 제공합니다. 또한 AmazonS3ReadOnlyAccess를 연결하여 빌드 아티팩트 다운로드에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeBuildReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 19:03 UTC
- 편집된 시간: 2020년 9월 14일, 16:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
```

```
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
```

```
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeCommitFullAccess

`AWSCodeCommitFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CodeCommit에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeCommitFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:02 UTC
- 편집된 시간: 2023년 7월 17일, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
```

```
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeCommitPowerUser

`AWSCodeCommitPowerUser`는 AWS 관리형 정책으로, AWS CodeCommit 리포지토리에 대한 전체 액세스를 제공하지만 리포지토리 삭제는 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeCommitPowerUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:06 UTC
- 편집된 시간: 2023년 7월 17일, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

정책 버전

정책 버전: v15(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
```

```
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
```

```
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
```

```
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeCommitReadOnly

`AWSCodeCommitReadOnly`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS CodeCommit에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeCommitReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:05 UTC
- 편집된 시간: 2021년 8월 18일, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
```

```
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess는 AWS 관리형 정책으로, 개정을 등록하고 배포할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployDeployerAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:18 UTC
- 편집된 시간: 2020년 4월 2일, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployFullAccess

AWSCodeDeployFullAccess는 AWS 관리형 정책으로, CodeDeploy 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:13 UTC
- 편집된 시간: 2020년 4월 2일, 16:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployReadOnlyAccess

`AWSCodeDeployReadOnlyAccess`는 AWS 관리형 정책으로, CodeDeploy 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeDeployReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 5월 19일, 18:21 UTC
- 편집된 시간: 2020년 4월 2일, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRole

AWSCodeDeployRole는 AWS 관리형 정책으로, 사용자를 대신하여 태그를 확장하고 Auto Scaling과 상호 작용할 수 있는 CodeDeploy 서비스 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 5월 4일, 18:05 UTC
- 편집된 시간: 2023년 8월 16일, 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRoleForCloudFormation

`AWSCodeDeployRoleForCloudFormation`는 AWS 관리형 정책으로, CloudFormation을 통해 블루/그린 배포를 수행하기 위해 사용자를 대신하여 Lambda 함수를 호출하는 CodeDeploy 서비스 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeDeployRoleForCloudFormation`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 5월 19일, 17:12 UTC
- 편집된 시간: 2020년 5월 19일, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRoleForECS

`AWSCodeDeployRoleForECS`는 AWS 관리형 정책으로, 사용자를 대신하여 ECS 블루/그린 배포를 수행할 수 있도록 CodeDeploy 서비스에 폭넓은 액세스를 제공합니다. 모든 S3 객체 읽기, 모든 Lambda 함수 호출, 계정 내 모든 SNS 주제에 게시, 모든 ECS 서비스 업데이트에 대한 전체 액세스와 같은 지원 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeDeployRoleForECS`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 20:40 UTC
- 편집된 시간: 2019년 9월 23일, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRoleForECSLimited

`AWSCodeDeployRoleForECSLimited`는 AWS 관리형 정책으로, 사용자를 대신하여 ECS 블루/그린 배포를 수행할 수 있도록 CodeDeploy 서비스에 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodeDeployRoleForECSLimited`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 20:42 UTC
- 편집된 시간: 2019년 9월 23일, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambda는 AWS 관리형 정책으로, 사용자를 대신하여 Lambda 배포를 수행할 수 있도록 CodeDeploy 서비스에 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForLambda를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 28일, 14:05 UTC
- 편집된 시간: 2019년 12월 3일, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeDeployRoleForLambdaLimited

AWSCodeDeployRoleForLambdaLimited는 AWS 관리형 정책으로, 사용자를 대신하여 Lambda 배포를 수행할 수 있도록 CodeDeploy 서비스에 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeDeployRoleForLambdaLimited를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 17일, 17:14 UTC
- 편집된 시간: 2020년 8월 17일, 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodePipeline_FullAccess

AWSCodePipeline_FullAccess는 를 AWS CodePipeline 통해 전체 액세스를 제공하는 AWS 관리형 AWS Management Console정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipeline_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 3일, 22:38 UTC
- 편집 시간: 2024년 3월 14일 17:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSCodePipeline_ReadOnlyAccess

`AWSCodePipeline_ReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console를 통해 AWS CodePipeline에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSCodePipeline_ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 3일, 22:25 UTC
- 편집된 시간: 2020년 8월 3일, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess는 AWS 관리형 정책으로, 모든 파이프라인의 수동 변경 사항을 보고 승인할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipelineApproverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 7월 28일, 18:59 UTC
- 편집된 시간: 2017년 8월 2일, 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess는 AWS 관리형 정책으로, 작업 세부 정보(임시 자격 증명 포함)를 폴링하고 AWS CodePipeline에 상태 업데이트를 보고하기 위해 사용자 지정 작업에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodePipelineCustomActionAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:02 UTC
- 편집된 시간: 2015년 7월 9일, 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeStarFullAccess

AWSCodeStarFullAccess는 AWS 관리형 정책으로, AWS Management Console를 통해 AWS CodeStar에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeStarFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 4월 19일, 16:23 UTC
- 편집된 시간: 2023년 3월 28일, 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicy는 AWS 관리형 정책으로, AWS CodeStar Notifications이 사용자를 대신하여 Amazon CloudWatch Events에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 5일, 16:10 UTC
- 편집된 시간: 2020년 3월 19일, 16:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCodeStarServiceRole

AWSCodeStarServiceRole는 AWS 관리형 정책으로, CodeStar가 고객을 대신하여 IAM 및 기타 서비스 리소스를 관리할 수 있도록 관리자 권한을 부여하는 DO NOT USE - AWS CodeStar 서비스 역할 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCodeStarServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 4월 19일, 15:20 UTC
- 편집된 시간: 2021년 9월 20일, 19:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine는 AWS 관리형 정책으로, IAM 사용자의 자격 증명이 침해되거나 공개적으로 노출된 경우 AWS 팀에서 적용하는 특정 작업에 대한 액세스를 거부합니다. 이 정책을 삭제하지 마십시오. 대신, 이 이벤트와 관련하여 귀하에게 전송된 이메일에 명시된 지침을 따르세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSCompromisedKeyQuarantine를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 11일, 18:04 UTC
- 편집된 시간: 2020년 8월 11일, 18:04 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2는 AWS 관리형 정책으로, IAM 사용자의 자격 증명이 침해되거나 공개적으로 노출된 경우 AWS 팀에서 적용하는 특정 작업에 대한 액세스를 거부합니다. 이 정책을 삭제하지 마십시오. 대신 이 이벤트와 관련하여 귀하를 위해 생성된 지원 사례에 명시된 지침을 따르세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSCompromisedKeyQuarantineV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 4월 21일, 22:30 UTC
- 편집된 시간: 2023년 3월 16일, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
```

```
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConfigMultiAccountSetupPolicy

`AWSConfigMultiAccountSetupPolicy`는 AWS 관리형 정책으로, Config가 AWS 서비스를 호출하고 조직 전체에 config 리소스를 배포할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 17일, 18:03 UTC
- 편집된 시간: 2023년 2월 24일, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy는 AWS 관리형 정책으로, AWS Config가 사용자를 대신하여 규정을 준수하지 않는 리소스를 수정할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 18일, 21:21 UTC
- 편집된 시간: 2019년 6월 18일, 21:21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConfigRoleForOrganizations

`AWSConfigRoleForOrganizations`는 AWS 관리형 정책으로, AWS Config가 읽기 전용 AWS Organizations API를 호출하도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSConfigRoleForOrganizations`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 3월 19일, 22:53 UTC
- 편집된 시간: 2020년 11월 24일, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConfigRulesExecutionRole

`AWSConfigRulesExecutionRole`는 AWS 관리형 정책으로, AWS Lambda 함수가 AWS Config API와 AWS Config가 Amazon S3에 정기적으로 전송하는 구성 스냅샷에 액세스할 수 있도록 허용합니다. 이 액세스는 사용자 지정 Config 규칙에 대한 구성 변경을 평가하는 함수에 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSConfigRulesExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 3월 25일, 17:59 UTC
- 편집된 시간: 2019년 5월 13일, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConfigServiceRolePolicy

`AWSConfigServiceRolePolicyConfig`가 사용자를 대신하여 AWS 서비스를 호출하고 리소스 구성을 수집하도록 허용하는 AWS 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 5월 30일, 23:31 UTC
- 편집 시간: 2024년 2월 22일 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

정책 버전

정책 버전: v50(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
```

```
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
```

```
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
```

```
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
```

```
            "cloudwatch:ListDashboards",
            "cloudwatch:ListMetricStreams",
            "cloudwatch:ListTagsForResource",
            "codeartifact:DescribeRepository",
            "codeartifact:GetRepositoryPermissionsPolicy",
            "codeartifact:ListDomains",
            "codeartifact:ListPackages",
            "codeartifact:ListPackageVersions",
            "codeartifact:ListRepositories",
            "codeartifact:ListTagsForResource",
            "codebuild:BatchGetReportGroups",
            "codebuild:ListReportGroups",
            "codecommit:GetRepository",
            "codecommit:GetRepositoryTriggers",
            "codecommit:ListRepositories",
            "codecommit:ListTagsForResource",
            "codedeploy:GetDeploymentConfig",
            "codeguru-profiler:DescribeProfilingGroup",
            "codeguru-profiler:GetNotificationConfiguration",
            "codeguru-profiler:GetPolicy",
            "codeguru-profiler:ListProfilingGroups",
            "codeguru-reviewer:DescribeRepositoryAssociation",
            "codeguru-reviewer:ListRepositoryAssociations",
            "codepipeline:GetPipeline",
            "codepipeline:GetPipelineState",
            "codepipeline:ListPipelines",
            "cognito-identity:DescribeIdentityPool",
            "cognito-identity:GetIdentityPoolRoles",
            "cognito-identity:GetPrincipalTagAttributeMap",
            "cognito-identity:ListIdentityPools",
            "cognito-identity:ListTagsForResource",
            "cognito-idp:DescribeIdentityProvider",
            "cognito-idp:DescribeResourceServer",
            "cognito-idp:DescribeUserPool",
            "cognito-idp:DescribeUserPoolClient",
            "cognito-idp:DescribeUserPoolDomain",
            "cognito-idp:GetGroup",
            "cognito-idp:GetUserPoolMfaConfig",
            "cognito-idp:ListGroups",
            "cognito-idp:ListIdentityProviders",
            "cognito-idp:ListResourceServers",
            "cognito-idp:ListTagsForResource",
            "cognito-idp:ListUserPoolClients",
            "cognito-idp:ListUserPools",
```

```
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
```

```
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
```

```
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTableReplicaAutoScaling",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:ListTables",
            "dynamodb:ListTagsOfResource",
            "ec2:Describe*",
            "ec2:DescribeClientVpnAuthorizationRules",
            "ec2:DescribeClientVpnEndpoints",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeFleets",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribePlacementGroups",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSpotFleetRequests",
            "ec2:DescribeTags",
            "ec2:DescribeTrafficMirrorFilters",
            "ec2:DescribeTrafficMirrorSessions",
            "ec2:DescribeTrafficMirrorTargets",
            "ec2:DescribeVolumeAttribute",
            "ec2:DescribeVolumes",
            "ec2:GetEbsEncryptionByDefault",
            "ec2:GetInstanceTypesFromInstanceRequirements",
            "ec2:GetIpamPoolAllocations",
            "ec2:GetIpamPoolCidrs",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
            "ec2:GetNetworkInsightsAccessScopeContent",
            "ecr-public:DescribeRepositories",
            "ecr-public:GetRepositoryCatalogData",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:ListTagsForResource",
            "ecr:BatchGetRepositoryScanningConfiguration",
            "ecr:DescribePullThroughCacheRules",
            "ecr:DescribeRegistry",
            "ecr:DescribeRepositories",
            "ecr:GetLifecyclePolicy",
            "ecr:GetRegistryPolicy",
            "ecr:GetRepositoryPolicy",
            "ecr:ListTagsForResource",
            "ecs:DescribeCapacityProviders",
```

```
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
```

```
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
```

```
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
```

```
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
```

```
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
```

```
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
```

```
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
```

```
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
```

```
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
```

```
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
```

```
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
```

```
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
```

```
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
```

```
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
```

```
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
```

```
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
```

```
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
```

```
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
```

```
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListImages",
            "sagemaker:ListImageVersions",
            "sagemaker:ListInferenceExperiments",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListPipelines",
            "sagemaker:ListProjects",
            "sagemaker:ListTags",
            "sagemaker:ListWorkteams",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
            "sdb:ListDomains",
            "secretsmanager:ListSecrets",
            "secretsmanager:ListSecretVersionIds",
            "securityhub:DescribeHub",
            "serviceCatalog:DescribePortfolioShares",
            "servicediscovery:GetInstance",
            "servicediscovery:GetNamespace",
            "servicediscovery:GetService",
            "servicediscovery:ListInstances",
            "servicediscovery:ListNamespaces",
            "servicediscovery:ListServices",
            "servicediscovery:ListTagsForResource",
            "ses:DescribeReceiptRule",
            "ses:DescribeReceiptRuleSet",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetEmailTemplate",
            "ses:GetTemplate",
            "ses:ListConfigurationSets",
            "ses:ListContactLists",
```

```
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
```

```
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
```

```
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSConfigUserAccess

AWSConfigUserAccess는 AWS 관리형 정책으로, 리소스에 대한 태그별 검색과 모든 태그 읽기를 포함하여 AWS Config를 사용할 수 있는 액세스를 제공합니다. 이러한 경우, 관리자 권한이 필요한 AWS Config를 구성할 권한을 제공하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSConfigUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 18일, 19:38 UTC
- 편집된 시간: 2019년 3월 18일, 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSConnector

AWSConnectorConnector가 사용자 대신 VM을 가져올 수 있도록 모든 EC2 객체에 대한 광범위한 읽기/쓰기 액세스, import-to-ec '2-'로 시작하는 S3 버킷에 대한 읽기/쓰기 액세스, 모든 S3 버킷을 나열하는 기능을 지원하는 AWS 관리형 정책입니다. AWS

이 정책 사용

사용자, 그룹 및 역할에 AWSConnector를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 11일, 17:14 UTC
- 편집된 시간: 2015년 9월 28일, 19:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSControlTowerAccountServiceRolePolicy

`AWSControlTowerAccountServiceRolePolicy`는 AWS 관리형 정책으로, AWS Control Tower가 사용자를 대신하여 자동화된 계정 구성 및 중앙 집중식 거버넌스를 제공하는 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 5일, 22:04 UTC
- 편집된 시간: 2023년 6월 5일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy는 AWS 관리형 정책으로, AWS Control Tower에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSControlTowerServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 5월 3일, 18:19 UTC
- 편집된 시간: 2023년 4월 12일, 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicy는 AWS 관리형 정책으로, 계정의 조직을 설명하고, MAP 프로그램을 위한 S3 버킷을 생성하여 태그를 적용하고, 비용 및 사용 보고서를 생성하고, 비용 및 사용 보고서 정의를 설명할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSCostAndUsageReportAutomationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 1일, 21:27 UTC
- 편집된 시간: 2021년 11월 1일, 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataExchangeFullAccess

AWSDataExchangeFullAccess는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 사용하여 AWS Data Exchange 및 AWS Marketplace 작업에 대한 전체 액세스를 부여합니다. 또한 AWS Data Exchange를 최대한 활용하는 데 필요한 관련 서비스에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDataExchangeFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2021년 12월 2일, 16:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
```

```
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataExchangeProviderFullAccess

`AWSDataExchangeProviderFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 사용하여 AWS Data Exchange 및 AWS Marketplace 작업에 대한 데이터 제공자 액세스를 부여합니다. 또한 AWS Data Exchange를 최대한 활용하는 데 필요한 관련 서비스에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataExchangeProviderFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2022년 3월 15일, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataExchangeReadOnly

`AWSDataExchangeReadOnly`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 사용하여 AWS Data Exchange 및 AWS Marketplace 작업에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataExchangeReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2021년 5월 10일, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
```

```
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataExchangeSubscriberFullAccess

`AWSDataExchangeSubscriberFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 사용하여 AWS Data Exchange 및 AWS Marketplace 작업에 대한 데이터 구독자 액세스를 부여합니다. 또한 AWS Data Exchange를 최대한 활용하는 데 필요한 관련 서비스에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataExchangeSubscriberFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 13일, 19:27 UTC
- 편집된 시간: 2021년 11월 29일, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataLifecycleManagerServiceRole

`AWSDataLifecycleManagerServiceRole`는 AWS 관리형 정책으로, AWS 리소스에 대한 조치를 취할 수 있도록 AWS Data Lifecycle Manager에 적절한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataLifecycleManagerServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 7월 6일, 19:34 UTC
- 편집된 시간: 2022년 9월 19일, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataLifecycleManagerServiceRoleForAMIManagement

`AWSDataLifecycleManagerServiceRoleForAMIManagement`는 AWS 관리형 정책으로, AMI 관리를 위해 AWS 리소스에 대한 조치를 취할 수 있도록 AWS Data Lifecycle Manager에 적절한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataLifecycleManagerServiceRoleForAMIManagement`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 10월 21일, 19:39 UTC
- 편집된 시간: 2021년 8월 19일, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataLifecycleManagerSSMFullAccess

`AWSDataLifecycleManagerSSMFullAccess`는 AWS 관리형 정책으로, 모든 Amazon EC2 인스턴스에서 사전 및 사후 스크립트를 실행하는 데 필요한 Systems Manager 작업을 수행할 수 있는 Amazon Data Lifecycle Manager 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataLifecycleManagerSSMFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 10월 31일, 20:29 UTC
- 편집 시간: 2023년 11월 16일 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataPipeline_FullAccess

`AWSDataPipeline_FullAccess`는 AWS 관리형 정책으로, Data Pipeline에 대한 전체 액세스 권한, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 목록 액세스 권한, 기본 역할에 대한 PassRole 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataPipeline_FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 19일, 23:14 UTC
- 편집된 시간: 2017년 8월 17일, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataPipeline_PowerUser

`AWSDataPipeline_PowerUser`는 AWS 관리형 정책으로, Data Pipeline에 대한 전체 액세스 권한, S3, DynamoDB, Redshift, RDS, SNS 및 IAM 역할에 대한 목록 액세스 권한, 기본 역할에 대한 PassRole 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataPipeline_PowerUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 19일, 23:16 UTC
- 편집된 시간: 2017년 8월 17일, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataSyncDiscoveryServiceRolePolicy

`AWSDataSyncDiscoveryServiceRolePolicy`는 AWS 관리형 정책으로, DataSync Discovery가 사용자를 대신하여 다른 AWS 서비스와 통합할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 20일, 22:19 UTC
- 편집된 시간: 2023년 3월 20일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDataSyncFullAccess

`AWSDataSyncFullAccess`종속성에 대한 전체 액세스를 제공하고 종속성에 대한 액세스를 AWS DataSync 최소화하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataSyncFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 19:40 UTC
- 편집 시간: 2024년 2월 16일 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSDataSyncReadOnlyAccess

`AWSDataSyncReadOnlyAccess`는 AWS 관리형 정책으로, AWS DataSync에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDataSyncReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 18일, 19:18 UTC
- 편집된 시간: 2020년 6월 30일, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepLensLambdaFunctionAccessPolicy

AWSDeepLensLambdaFunctionAccessPolicy는 AWS 관리형 정책으로, 이 정책은 DeepLens 디바이스에서 실행되는 DeepLens 관리 Lambda 함수에 필요한 권한을 지정합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepLensLambdaFunctionAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 15:47 UTC
- 편집된 시간: 2019년 6월 11일, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepLensServiceRolePolicy

AWSDeepLensServiceRolePolicy는 AWS 관리형 정책으로, DeepLens 및 IoT, S3, GreenGrass, AWS Lambda를 포함한 종속성에서 필요한 AWS 서비스, 리소스, 역할에 대한 AWS DeepLens 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepLensServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 11월 29일, 15:46 UTC
- 편집된 시간: 2019년 9월 25일, 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess는 AWS 관리형 정책으로, 다중 사용자 모드와 단일 사용자 모드 간 전환을 포함한 모든 작업에 대한 DeepRacer 관리자 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerAccountAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 28일, 01:27 UTC
- 편집된 시간: 2021년 10월 28일, 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerCloudFormationAccessPolicy

`AWSDeepRacerCloudFormationAccessPolicy`는 AWS 관리형 정책으로, CloudFormation이 사용자를 대신하여 AWS 스택과 리소스를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDeepRacerCloudFormationAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 2월 28일, 21:59 UTC
- 편집된 시간: 2019년 6월 14일, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess는 AWS 관리형 정책으로, DeepRacer 다중 사용자 모드에서 DeepRacer를 사용하기 위한 기본 사용자 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerDefaultMultiUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 28일, 01:27
- 편집된 시간: 2021년 10월 28일, 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerFullAccess

`AWSDeepRacerFullAccess`는 AWS 관리형 정책으로, AWS DeepRacer에 대한 전체 액세스를 제공합니다. 또한 관련 서비스(예: S3)에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDeepRacerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 5일, 22:03 UTC
- 편집된 시간: 2020년 10월 5일, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicy는 AWS 관리형 정책으로, RoboMaker가 사용자를 대신하여 필요한 리소스를 생성하고 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerRoboMakerAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 2월 28일, 21:59 UTC
- 편집된 시간: 2019년 2월 28일, 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy는 AWS 관리형 정책으로, DeepRacer가 사용자를 대신하여 필요한 리소스를 생성하고 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeepRacerServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 2월 28일, 21:58 UTC
- 편집된 시간: 2019년 6월 12일, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDenyAll

AWSDenyAll는 AWS 관리형 정책으로, 모든 액세스를 거부합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDenyAll를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 1일, 22:36 UTC

- 편집 시간: 2023년 12월 18일 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeviceFarmFullAccess

`AWSDeviceFarmFullAccess`는 AWS 관리형 정책으로, 모든 AWS Device Farm 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDeviceFarmFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 13일, 16:37 UTC
- 편집된 시간: 2015년 7월 13일, 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeviceFarmServiceRolePolicy

AWSDeviceFarmServiceRolePolicy는 AWS 관리형 정책으로, AWS Device Farm에 사용자를 대신하여 EC2 Network API를 호출할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 20일, 21:02 UTC
- 편집된 시간: 2022년 9월 20일, 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy는 AWS 관리형 정책으로, AWS Device Farm에 사용자를 대신하여 EC2 API를 호출할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 5월 26일, 22:01 UTC
- 편집된 시간: 2021년 5월 26일, 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDirectConnectFullAccess

`AWSDirectConnectFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Direct Connect에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectConnectFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 4월 30일, 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDirectConnectReadOnlyAccess

AWSDirectConnectReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Direct Connect에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDirectConnectReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2020년 5월 18일, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDirectConnectServiceRolePolicy

`AWSDirectConnectServiceRolePolicy`는 AWS 관리형 정책으로, 사용자를 대신하여 AWS 리소스를 생성하고 관리할 수 있는 AWS Direct Connect 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 1월 14일, 18:35 UTC
- 편집된 시간: 2021년 1월 14일, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDirectoryServiceFullAccess

`AWSDirectoryServiceFullAccess`는 AWS 관리형 정책으로, AWS Directory Service에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDirectoryServiceFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2020년 11월 24일, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDirectoryServiceReadOnlyAccess

`AWSDirectoryServiceReadOnlyAccess`는 AWS 관리형 정책으로, AWS Directory Service에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSDirectoryServiceReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2018년 9월 25일, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDiscoveryContinuousExportFirehosePolicy

`AWSDiscoveryContinuousExportFirehosePolicy`는 AWS 관리형 정책으로, AWS Discovery Continuous Export에 필요한 AWS 리소스에 대한 쓰기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSDiscoveryContinuousExportFirehosePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 8월 9일, 18:29 UTC
- 편집된 시간: 2021년 6월 8일, 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicy는 AWS 관리형 정책으로, DMS Fleet Advisor가 사용자를 대신하여 CloudWatch 지표를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2023년 3월 6일, 09:10 UTC
- 편집된 시간: 2023년 3월 6일, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSDMSServerlessServiceRolePolicy

`AWSDMSServerlessServiceRolePolicy`는 AWS 관리형 정책으로, AWS DMS Serverless에 사용자를 대신하여 사용자 계정에서 DMS 리소스를 생성하고 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 18일, 20:28 UTC
- 편집된 시간: 2023년 5월 18일, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
```

```
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy는 AWS 관리형 정책으로, EC2 CapacityReservation Fleet 서비스가 용량 예약을 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 29일, 14:43 UTC
- 편집된 시간: 2021년 9월 29일, 14:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy는 AWS 관리형 정책으로, EC2 Fleet이 인스턴스를 시작하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 21일, 00:08 UTC
- 편집된 시간: 2020년 5월 4일, 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEC2SpotFleetServiceRolePolicy

`AWSEC2SpotFleetServiceRolePolicy`는 AWS 관리형 정책으로, EC2 Spot Fleet이 스팟 플릿 인스턴스를 시작하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 23일, 19:13 UTC
- 편집된 시간: 2020년 3월 16일, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy는 AWS 관리형 정책으로, EC2 Spot이 스팟 인스턴스를 시작하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 18일, 18:51 UTC
- 편집된 시간: 2018년 12월 12일, 00:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSECRPullThroughCache_ServiceRolePolicy

AWSECRPullThroughCache_ServiceRolePolicy는 AWS 관리형 정책으로, AWS ECR 풀 스루 캐시에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 26일, 21:51 UTC
- 편집된 시간: 2023년 11월 13일, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkCustomPlatformforEC2Role

`AWSElasticBeanstalkCustomPlatformforEC2Role`는 AWS 관리형 정책으로, 사용자 지정 플랫폼 빌더 환경의 인스턴스에 EC2 인스턴스를 시작하고, EBS 스냅샷 및 AMI를 생성하고, 로그를 Amazon CloudWatch Logs로 스트리밍하고, Amazon S3에 아티팩트를 저장할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkCustomPlatformforEC2Role`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 2월 21일, 22:50 UTC
- 편집된 시간: 2017년 2월 21일, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkEnhancedHealth

AWSElasticBeanstalkEnhancedHealth는 AWS 관리형 정책으로, Health Monitoring system에 대한 AWS Elastic Beanstalk Service 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkEnhancedHealth를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 8일, 23:17 UTC
- 편집된 시간: 2018년 4월 9일, 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkMaintenance

`AWSElasticBeanstalkMaintenance`는 AWS 관리형 정책으로, 유지 관리 목적으로 사용자를 대신하여 리소스를 업데이트할 수 있는 제한된 권한을 부여하는 AWS Elastic Beanstalk 서비스 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 1월 11일, 23:22 UTC
- 편집된 시간: 2019년 6월 4일, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
```

```
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Beanstalk 환경의 관리형 업데이트를 수행하는 데 사용되는 Elastic Beanstalk 서비스 역할을 위한 정책입니다. 이 정책은 다른 사용자나 역할에 연결되어서는 안 됩니다. 이 정책은 AutoScaling, EC2, ECS, Elastic Load Balancing 및 CloudFormation을 포함한 다양한 AWS 서비스에서 리소스를 생성하고 관리할 수 있는 광범위한 권한을 부여합니다. 또한 이 정책은 해당 서비스에 사용할 수 있는 모든 IAM 역할의 전달을 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 3일, 22:18 UTC
- 편집된 시간: 2023년 3월 23일, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy는 AWS 관리형 정책으로, 관리형 업데이트에 제한된 권한을 부여하는 AWS Elastic Beanstalk 서비스 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 21일, 22:35 UTC
- 편집된 시간: 2023년 3월 24일, 00:18 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
```

```
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
```

```
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
```

```
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDocker는 AWS 관리형 정책으로, Amazon EC2 Container Service를 사용하여 컨테이너 배포 태스크를 관리할 수 있도록 멀티컨테이너 Docker 환경의 인스턴스에 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkMulticontainerDocker를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:15 UTC
- 편집된 시간: 2023년 3월 23일, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly는 AWS 관리형 정책으로, 읽기 전용 권한을 부여합니다. 운영자가 AWS Elastic Beanstalk 애플리케이션과 관련된 리소스에 대한 정보를 검색할 수 있는 직접 액세스를 명시적으로 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 19:02 UTC
- 편집된 시간: 2021년 1월 22일, 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore는 AWS 관리형 정책으로, AWSElasticBeanstalkRoleCore(Elastic Beanstalk 작업 역할)는 웹 서비스 환경의 핵심 작업을 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleCore를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:48 UTC
- 편집된 시간: 2020년 9월 9일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleCWL

`AWSElasticBeanstalkRoleCWL`는 AWS 관리형 정책으로, 환경에서 Amazon CloudWatch Logs 로그 그룹을 관리할 수 있도록 허용하는 관리형 정책(Elastic Beanstalk 작업 역할)입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkRoleCWL`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:49 UTC

- 편집된 시간: 2020년 6월 5일, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS는 AWS 관리형 정책으로, (Elastic Beanstalk 작업 역할) 멀티컨테이너 Docker 환경에서 Amazon ECS 클러스터를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleECS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:47 UTC
- 편집된 시간: 2023년 3월 23일, 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleRDS

`AWSElasticBeanstalkRoleRDS`는 AWS 관리형 정책으로, (Elastic Beanstalk 작업 역할)환경에서 Amazon RDS 인스턴스를 통합할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkRoleRDS`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2020년 6월 5일, 21:46 UTC
- 편집된 시간: 2020년 6월 5일, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS는 AWS 관리형 정책으로, (Elastic Beanstalk 작업 역할)환경에서 Amazon SNS 주제 통합을 활성화할 수 있도록 허용하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkRoleSNS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 6월 5일, 21:46 UTC
- 편집된 시간: 2020년 6월 5일, 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkRoleWorkerTier

`AWSElasticBeanstalkRoleWorkerTier`는 AWS 관리형 정책으로, (Elastic Beanstalk 작업 역할) 작업자 환경 티어가 Amazon DynamoDB 테이블과 Amazon SQS 대기열을 생성할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkRoleWorkerTier`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2020년 6월 5일, 21:43 UTC
- 편집된 시간: 2020년 6월 5일, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkService

`AWSElasticBeanstalkService`는 AWS 관리형 정책으로, 이 정책은 사용 중단 중입니다. 지침은 설명서를 참조하세요. https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS 사용자를 대신하여 리소스(예: AutoScaling, EC2, S3, CloudFormation, ELB 등)를 생성하고 관리할 수 있는 권한을 부여하는 Elastic Beanstalk 서비스 역할 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticBeanstalkService`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 4월 11일, 20:27 UTC
- 편집된 시간: 2023년 5월 10일, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkServiceRolePolicy

`AWSElasticBeanstalkServiceRolePolicy`는 AWS 관리형 정책으로, 사용자를 대신하여 리소스(예: AutoScaling, EC2, S3, CloudFormation, ELB 등)를 생성하고 관리할 수 있는 권한을 부여하는 AWS Elastic Beanstalk 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 13일, 23:46 UTC
- 편집된 시간: 2019년 6월 6일, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier는 AWS 관리형 정책으로, 웹 서버 환경의 인스턴스에 로그 파일을 Amazon S3에 업로드할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkWebTier를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:08 UTC
- 편집된 시간: 2020년 9월 9일, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTier는 AWS 관리형 정책으로, 작업자 환경의 인스턴스에 Amazon S3에 로그 파일을 업로드하고, Amazon SQS를 사용하여 애플리케이션의 작업 대기열을 모니터링하고, Amazon DynamoDB를 사용하여 리더 선출을 수행하고, Amazon CloudWatch에 상태 모니터링을 위한 지표를 게시할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticBeanstalkWorkerTier를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 2월 8일, 23:12 UTC
- 편집된 시간: 2020년 9월 9일, 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryAgentInstallationPolicy

AWSElasticDisasterRecoveryAgentInstallationPolicy는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)와 함께 외부 서버를 AWS로 복구하기 위해 사용되는 AWS Replication Agent를 설치할 수 있도록 허용합니다. 이 정책을 AWS Replication Agent의 설치 단계에서 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryAgentInstallationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:37 UTC
- 편집 시간: 2023년 11월 27일 12:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryAgentPolicy

`AWSElasticDisasterRecoveryAgentPolicy`는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)와 함께 소스 서버를 AWS로 복구하기 위해 사용되는 AWS Replication Agent를 사용할 수 있도록 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryAgentPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:32 UTC
- 편집 시간: 2023년 11월 27일 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryConsoleFullAccess

`AWSElasticDisasterRecoveryConsoleFullAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)의 모든 퍼블릭 API에 대한 전체 액세스 권한과 KMS 키, License Manager, Resource Groups, Elastic Load Balancing, IAM 및 EC2 정보를 읽을 수 있는 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:46 UTC
- 편집된 시간: 2023년 10월 16일, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryConsoleFullAccess_v2

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`는 다음과 같은 AWS관리형 정책입니다. 이 정책은 DRS (AWSElastic Disaster Recovery) 의 모든 퍼블릭 API와 AWS DRS 콘솔에서 사용하는 다른 AWS 서비스의 모든 퍼블릭 API에 대한 전체 액세스를 제공하는 관리형 정책입니다. AWS 이 정책을 사용자 또는 역할에 연결하십시오.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryConsoleFullAccess_v2`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 27일 13:35 UTC
- 편집 시간: 2023년 11월 27일, 13:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
```

```
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryConversionServerPolicy

`AWSElasticDisasterRecoveryConversionServerPolicy`는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery 변환 서버의 인스턴스 역할에 연결됩니다. 이 정책은 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Conversion Servers가 DRS 서비스와 통신할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 DRS에 의해 (EC2 Instance Profile로) DRS Conversion Servers에 연결되며, 필요할 때 DRS에 의해 자동으로 시작되고 종료됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다. DRS Conversion Servers는 사용자가 DRS 콘솔, CLI 또는 API를 사용하여 소스 서버를 복구하도록 선택할 때 Elastic Disaster Recovery에서 사용됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryConversionServerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 13:42 UTC
- 편집 시간: 2023년 11월 27일 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)가 교차 계정 복제 및 교차 계정 페일백을 지원할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryCrossAccountReplicationPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 5월 14일, 07:16 UTC
- 편집 시간: 2024년 1월 17일 13:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryEc2InstancePolicy

`AWSElasticDisasterRecoveryEc2InstancePolicy`는 AWS 관리형 정책으로, 이 정책은 EC2(교차 리전 또는 교차 AZ)에서 실행되는 소스 서버를 복구하기 위해 AWS Elastic Disaster Recovery(DRS)에서 사용되는 AWS Replication Agent를 설치하고 사용할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 EC2 Instances에 (EC2 Instance Profile로) 연결되어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryEc2InstancePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 5월 26일, 12:30 UTC
- 편집 시간: 2023년 11월 27일 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryFailbackInstallationPolicy

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`정책을 IAM ID에 연결할 수 있는 AWS 관리형 AWSElasticDisasterRecoveryFailbackInstallationPolicy 정책입니다. 이 정책을 사용하면 Recovery Instances를 원래 소스 인프라로 페일백하는 데 사용되는 Elastic Disaster Recovery Failback Client를 설치할 수 있습니다. Elastic Disaster Recovery Failback Client를 실행할 때 보안 인증 정보를 제공한 IAM 사용자 또는 역할에 이 정책을 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryFailbackInstallationPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 11:02 UTC

- 편집 시간: 2023년 11월 27일 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryFailbackPolicy

`AWSElasticDisasterRecoveryFailbackPolicy`는 AWS 관리형 정책으로, 이 정책은 Recovery Instances를 원래 소스 인프라로 페일백하는 데 사용되는 Elastic Disaster Recovery Failback Client를 사용할 수 있도록 허용합니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryFailbackPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:41 UTC
- 편집 시간: 2023년 11월 27일 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryLaunchActionsPolicy

`AWSElasticDisasterRecoveryLaunchActionsPolicy`는 AWS 관리형 정책으로, 이 정책은 Amazon SSM 및 추가 서비스를 사용하여 AWS Elastic Disaster Recovery(AWSDRS)에서 시작 후 작업을 실행하는 데 필요한 권한을 허용합니다. 이 정책을 IAM 역할 또는 사용자에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryLaunchActionsPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 9월 13일, 07:38 UTC
- 편집된 시간: 2023년 10월 16일, 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
```

```
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryNetworkReplicationPolicy

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`는 AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)가 네트워크 복제를 지원하도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryNetworkReplicationPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 11일, 12:36 UTC
- 편집 시간: 2024년 1월 2일 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryReadOnlyAccess

`AWSElasticDisasterRecoveryReadOnlyAccess`정책을 IAM ID에 연결할 수 있는 AWS 관리형 AWSElasticDisasterRecoveryReadOnlyAccess 정책입니다. 이 정책은 DRS(Elastic Disaster

Recovery)의 모든 읽기 전용 퍼블릭 API와 DRS 콘솔을 완전히 읽기 전용으로 사용하는 데 필요한 기타 AWS 서비스의 일부 읽기 전용 API에 대한 권한을 제공합니다. 이 정책을 IAM 사용자 또는 역할에 연결하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 17일, 10:50 UTC
- 편집 시간: 2023년 11월 27일, 13:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
```

```
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryRecoveryInstancePolicy

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`는 AWS 관리형 정책으로, 이 정책은 Elastic Disaster Recovery의 Recovery Instance의 역할에 연결됩니다. 이 정책을 사용하면 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Recovery Instance

가 DRS 서비스와 통신하고 원래 소스 인프라로 페일백할 수 있습니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery를 통해 (EC2 Instance Profile로) DRS Recovery Instances에 연결됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryRecoveryInstancePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 10:20 UTC
- 편집 시간: 2023년 11월 27일 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryReplicationServerPolicy

`AWSElasticDisasterRecoveryReplicationServerPolicy`는 AWS 관리형 정책으로, 이 정책은 Elastic Disaster Recovery Replication 서버의 인스턴스 역할에 연결됩니다. 이 정책은 Elastic Disaster Recovery에서 시작하는 EC2 인스턴스인 Elastic Disaster Recovery(DRS) Replication Servers가 DRS 서비스와 통신하고 AWS 계정에 EBS 스냅샷을 생성할 수 있도록 허용합니다. 이 정책이 있는 IAM 역할은 Elastic Disaster Recovery에 의해 필요에 따라 DRS에 의해 자동으로 시작 및 종료되는 DRS Replication Servers에 (EC2 Instance Profile로) 연결됩니다. DRS Replication Servers는 DRS에서 관리하는 복구 프로세스의 일환으로 외부 서버에서 AWS로의 데이터 복제를 용이하게 하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryReplicationServerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 11월 17일, 13:34 UTC
- 편집 시간: 2023년 11월 27일 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryServiceRolePolicy

`AWSElasticDisasterRecoveryServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 Elastic Disaster Recovery가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 10:56 UTC
- 편집 시간: 2024년 1월 17일 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
```

```
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy는 AWS 관리형 정책으로, 이 정책은 소스 서버 및 작업과 같은 AWS Elastic Disaster Recovery(DRS) 리소스에 대한 읽기 전용 액세스를 허용합니다. 또한 변환된 스냅샷을 생성하고 해당 EBS 스냅샷을 특정 계정과 공유할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElasticDisasterRecoveryStagingAccountPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 5월 26일, 09:49 UTC
- 편집 시간: 2023년 11월 27일, 13:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2` AWS 관리형 정책으로, 이 정책은 AWS Elastic Disaster Recovery(DRS)에서 소스 서버를 별도의 대상 계정으로 복구하고 페일백을 허용하는 데 사용됩니다. 이 정책을 IAM 사용자 또는 역할에 연결하지 않는 것이 좋습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElasticDisasterRecoveryStagingAccountPolicy_v2`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2023년 1월 5일, 12:11 UTC
- 편집 시간: 2023년 11월 27일 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticLoadBalancingClassicServiceRolePolicy

`AWSElasticLoadBalancingClassicServiceRolePolicy`는 AWS 관리형 정책으로, AWS Elastic Load Balancing 컨트롤 플레인 - Classic에 대한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 19일, 22:36 UTC

- 편집된 시간: 2019년 10월 7일, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElasticLoadBalancingServiceRolePolicy

`AWSElasticLoadBalancingServiceRolePolicy`는 AWS 관리형 정책으로, AWS Elastic Load Balancing 컨트롤 플레인에 대한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 19일, 22:19 UTC
- 편집된 시간: 2021년 8월 26일, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaConvertFullAccess

`AWSElementalMediaConvertFullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 AWS Elemental MediaConvert에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaConvertFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 25일, 19:25 UTC
- 편집된 시간: 2019년 6월 10일, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaConvertReadOnly

`AWSElementalMediaConvertReadOnly`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 AWS Elemental MediaConvert에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaConvertReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 25일, 19:25 UTC
- 편집된 시간: 2019년 6월 10일, 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaLiveFullAccess

`AWSElementalMediaLiveFullAccess`는 AWS 관리형 정책으로, AWS Elemental MediaLive 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaLiveFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 8일, 17:07 UTC
- 편집된 시간: 2020년 7월 8일, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaLiveReadOnly

`AWSElementalMediaLiveReadOnly`는 AWS 관리형 정책으로, AWS Elemental MediaLive 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaLiveReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 7월 8일, 16:38 UTC
- 편집된 시간: 2020년 7월 8일, 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaPackageFullAccess

`AWSElementalMediaPackageFullAccess`는 AWS 관리형 정책으로, AWS Elemental MediaPackage 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaPackageFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 12월 29일, 23:39 UTC
- 편집된 시간: 2017년 12월 29일, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaPackageReadOnly

`AWSElementalMediaPackageReadOnly`는 AWS 관리형 정책으로, AWS Elemental MediaPackage 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaPackageReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2017년 12월 30일, 00:04 UTC
- 편집된 시간: 2017년 12월 30일, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaPackageV2FullAccess

`AWSElementalMediaPackageV2FullAccess`는 AWS 관리형 정책으로, AWS Elemental MediaPackageV2 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaPackageV2FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 20:29 UTC
- 편집된 시간: 2023년 7월 25일, 20:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaPackageV2ReadOnly

AWSElementalMediaPackageV2ReadOnly는 AWS 관리형 정책으로, AWS Elemental MediaPackageV2 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaPackageV2ReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 20:31 UTC
- 편집된 시간: 2023년 7월 25일, 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaStoreFullAccess

`AWSElementalMediaStoreFullAccess`는 AWS 관리형 정책으로, 모든 MediaStore API에 대한 전체 읽기 및 쓰기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaStoreFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 5일, 23:15 UTC
- 편집된 시간: 2018년 3월 5일, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaStoreReadOnly

`AWSElementalMediaStoreReadOnly`는 AWS 관리형 정책으로, MediaStore API에 대한 읽기 전용 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaStoreReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 8일, 19:48 UTC
- 편집된 시간: 2018년 3월 8일, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaTailorFullAccess

AWSElementalMediaTailorFullAccess는 AWS 관리형 정책으로, AWS Elemental MediaTailor 리소스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSElementalMediaTailorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 23일, 00:04 UTC
- 편집된 시간: 2021년 11월 23일, 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSElementalMediaTailorReadOnly

`AWSElementalMediaTailorReadOnly`는 AWS 관리형 정책으로, AWS Elemental MediaTailor 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSElementalMediaTailorReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 23일, 00:05 UTC
- 편집된 시간: 2021년 11월 23일, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEnhancedClassicNetworkingMangementPolicy

AWSEnhancedClassicNetworkingMangementPolicy는 AWS 관리형 정책으로, 향상된 클래식 네트워킹 관리 기능을 활성화하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 9월 20일, 17:29 UTC
- 편집된 시간: 2017년 9월 20일, 17:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess`는 AWS 관리형 정책으로, AWS Entity Resolution 및 관련 서비스에 대한 콘솔 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSEntityResolutionConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 17일, 17:54 UTC
- 편집된 시간: 2023년 10월 16일, 18:46 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Entity Resolution에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSEntityResolutionConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 17일, 18:18 UTC
- 편집된 시간: 2023년 8월 17일, 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorEC2Access

`AWSFaultInjectionSimulatorEC2Access`는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 EC2 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSFaultInjectionSimulatorEC2Access`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:39 UTC
- 편집 시간: 2023년 11월 27일 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorECSAccess

`AWSFaultInjectionSimulatorECSAccess`는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 ECS 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSFaultInjectionSimulatorECSAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2022년 10월 26일, 20:37 UTC
- 편집 시간: 2024년 1월 25일 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorEKSAccess

`AWSFaultInjectionSimulatorEKSAccess`는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 EKS 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSFaultInjectionSimulatorEKSAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:34 UTC
- 편집된 시간: 2023년 11월 13일, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorNetworkAccess

`AWSFaultInjectionSimulatorNetworkAccess`는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 EC2 네트워킹 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSFaultInjectionSimulatorNetworkAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:32 UTC
- 편집 시간: 2024년 1월 25일 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 RDS 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorRDSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 20:30 UTC
- 편집된 시간: 2023년 11월 13일, 16:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess는 AWS 관리형 정책으로, 이 정책은 FIS 작업을 수행하기 위해 SSM 및 기타 필요한 서비스에 Fault Injection Simulator 서비스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFaultInjectionSimulatorSSMAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 10월 26일, 15:33 UTC
- 편집된 시간: 2023년 6월 2일, 22:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicyAmazon에서 사용하거나 AWS관리하는 리소스 AWS 서비스 및 액세스를 가능하게 하는 정책인 관리형 정책입니다. FinSpace

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 12일, 16:42 UTC
- 편집 시간: 2023년 12월 1일 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFMAdminFullAccess

AWSFMAdminFullAccess는 AWS 관리형 정책으로, AWS FM 관리자에 대한 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFMAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 18:06 UTC
- 편집된 시간: 2022년 10월 20일, 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess는 AWS 관리형 정책으로, AWS FM 작업을 모니터링할 수 있는 AWS FM 관리자를 위한 읽기 전용 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSFMAdminReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 20:07 UTC
- 편집된 시간: 2022년 10월 31일, 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSFMMemberReadOnlyAccess

`AWSFMMemberReadOnlyAccess`는 AWS 관리형 정책으로, AWS Firewall Manager 멤버 계정에 대한 AWS WAF 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSFMMemberReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 9일, 21:05 UTC
- 편집된 시간: 2018년 5월 9일, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSForWordPressPluginPolicy

`AWSForWordPressPluginPolicy`는 AWS 관리형 정책으로, AWS For Wordpress 플러그인에 대한 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSForWordPressPluginPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 10월 30일, 00:27 UTC
- 편집된 시간: 2020년 1월 20일, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGitSyncServiceRolePolicy

`AWSGitSyncServiceRolePolicy`는 AWS 관리형 정책으로, AWS Code Connections가 git 저장소의 콘텐츠를 동기화할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 16일, 17:05 UTC
- 편집된 시간: 2023년 11월 16일, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlobalAcceleratorSLRPolicy

`AWSGlobalAcceleratorSLRPolicy`는 AWS 관리형 정책으로, AWS Global Accelerator에 EC2 Elastic 네트워크 인터페이스 및 보안 그룹을 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 4월 5일, 19:39 UTC
- 편집된 시간: 2023년 9월 12일, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueConsoleFullAccess

AWSGlueConsoleFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Glue에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 7월 14일, 14:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueConsoleSageMakerNotebookFullAccess

AWSGlueConsoleSageMakerNotebookFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Glue에 대한 전체 액세스와 SageMaker 노트북 인스턴스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueConsoleSageMakerNotebookFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 5일, 17:52 UTC
- 편집된 시간: 2021년 7월 15일, 15:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AwsGlueDataBrewFullAccessPolicy

AwsGlueDataBrewFullAccessPolicy는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Glue DataBrew에 대한 전체 액세스를 제공합니다. 또한 관련 서비스(예: S3, KMS, Glue)에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueDataBrewFullAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 11일, 16:51 UTC
- 편집된 시간: 2022년 2월 4일, 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueDataBrewServiceRole

AWSGlueDataBrewServiceRole는 AWS 관리형 정책으로, 이 정책은 사용자의 Glue 데이터 카탈로그에 대한 작업을 수행할 수 있는 권한을 부여하고, 또한 Glue가 ENI를 생성하여 VPC의 리소스에 연결하도록 허용하는 ec2 작업에 대한 권한을 제공하고, Glue가 lakeformation에 등록된 데이터에 액세스할 수 있도록 허용하고, 사용자의 Cloudwatch에 액세스할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGlueDataBrewServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 4일, 21:26 UTC
- 편집 시간: 2024년 3월 20일 23:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSGlueSchemaRegistryFullAccess

`AWSGlueSchemaRegistryFullAccess`는 AWS 관리형 정책으로, AWS Glue Schema Registry Service에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGlueSchemaRegistryFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 00:19 UTC

- 편집된 시간: 2020년 11월 20일, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueSchemaRegistryReadonlyAccess

`AWSGlueSchemaRegistryReadonlyAccess`는 AWS 관리형 정책으로, AWS Glue Schema Registry Service에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGlueSchemaRegistryReadonlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 20일, 00:20 UTC

- 편집된 시간: 2020년 11월 20일, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueServiceNotebookRole

`AWSGlueServiceNotebookRole`는 AWS 관리형 정책으로, 고객이 노트북 서버를 관리할 수 있도록 하는 AWS Glue 서비스 역할에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGlueServiceNotebookRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 10월 9일, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGlueServiceRole

`AWSGlueServiceRole`는 AWS 관리형 정책으로, EC2, S3, Cloudwatch Logs를 포함한 관련 서비스에 대한 액세스를 허용하는 AWS Glue 서비스 역할에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGlueServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:37 UTC
- 편집된 시간: 2023년 9월 11일, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy는 AWS 관리형 정책으로, 사용자가 자신과 연관된 노트북 세션만 생성하고 사용할 수 있도록 허용하는 권한을 제공합니다. 이 정책에는 제한된 Glue 세션 역할을 사용자가 전달할 수 있도록 명시적으로 허용하는 권한도 포함되어 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedNotebookPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 18일, 15:24 UTC
- 편집 시간: 2023년 11월 22일 01:32 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AwsGlueSessionUserRestrictedNotebookServiceRole

`AwsGlueSessionUserRestrictedNotebookServiceRole`는 AWS 관리형 정책으로, 세션을 제외한 모든 AWS Glue 리소스에 대한 전체 액세스를 제공합니다. 사용자가 자신과 연결된 노트북 세션만 생성하고 사용할 수 있도록 허용합니다. 이 정책에는 AWS Glue에서 다른 AWS 서비스의 Glue 리소스를 관리하는 데 필요한 기타 권한도 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AwsGlueSessionUserRestrictedNotebookServiceRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 18일, 15:27 UTC
- 편집된 시간: 2022년 4월 18일, 15:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
```

```
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AwsGlueSessionUserRestrictedPolicy

`AwsGlueSessionUserRestrictedPolicy`는 AWS 관리형 정책으로, 사용자가 자신과 연관된 대화형 세션만 생성하고 사용할 수 있도록 허용하는 권한을 제공합니다. 이 정책에는 제한된 Glue 세션 역할을 사용자가 전달할 수 있도록 명시적으로 허용하는 권한도 포함되어 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AwsGlueSessionUserRestrictedPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 14일, 21:31 UTC
- 편집된 시간: 2022년 4월 14일, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AwsGlueSessionUserRestrictedServiceRole

`AwsGlueSessionUserRestrictedServiceRole`는 AWS 관리형 정책으로, 세션을 제외한 모든 AWS Glue 리소스에 대한 전체 액세스를 제공합니다. 사용자와 연결된 대화형 세션만 사용자가 생성하고 사용할 수 있도록 허용합니다. 이 정책에는 AWS Glue에서 다른 AWS 서비스의 Glue 리소스를 관리하는 데 필요한 기타 권한도 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AwsGlueSessionUserRestrictedServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2022년 4월 14일, 21:30 UTC
- 편집된 시간: 2022년 4월 14일, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGrafanaAccountAdministrator

`AWSGrafanaAccountAdministrator`는 AWS 관리형 정책으로, Amazon Grafana 내에서 조직 전체를 위한 작업 공간을 생성하고 관리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGrafanaAccountAdministrator`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:20 UTC
- 편집된 시간: 2022년 2월 15일, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGrafanaConsoleReadOnlyAccess

`AWSGrafanaConsoleReadOnlyAccess`는 AWS 관리형 정책으로, Amazon Grafana의 읽기 전용 작업에 대한 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGrafanaConsoleReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:10 UTC
- 편집된 시간: 2022년 2월 15일, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGrafanaWorkspacePermissionManagement

`AWSGrafanaWorkspacePermissionManagement`는 AWS 관리형 정책으로, AWS Grafana workspaces에 대한 사용자 및 그룹 권한을 업데이트하는 기능만 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGrafanaWorkspacePermissionManagement를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 23일, 00:15 UTC
- 편집된 시간: 2023년 3월 15일, 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGrafanaWorkspacePermissionManagementV2

`AWSGrafanaWorkspacePermissionManagementV2`Amazon AWSManaged Grafana 작업 영역에 대한 IAM ID 센터 (IdC) 사용자 및 그룹 권한을 업데이트하는 기능을 제공하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGrafanaWorkspacePermissionManagementV2`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2024년 1월 5일 18:39 UTC

- 편집 시간: 2024년 1월 5일 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGreengrassFullAccess

AWSGreengrassFullAccess는 AWS 관리형 정책으로, 이 정책은 AWS Greengrass 구성, 관리 및 배포 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGreengrassFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 5월 3일, 00:47 UTC
- 편집된 시간: 2017년 5월 3일, 00:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGreengrassReadOnlyAccess

`AWSGreengrassReadOnlyAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Greengrass 구성, 관리 및 배포 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSGreengrassReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 30일, 16:01 UTC
- 편집된 시간: 2018년 10월 30일, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGreengrassResourceAccessRolePolicy

`AWSGreengrassResourceAccessRolePolicy`는 AWS 관리형 정책으로, AWS Lambda 및 AWS IoT 사물 섀도우를 포함한 관련 서비스에 대한 액세스를 허용하는 AWS Greengrass 서비스 역할에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGreengrassResourceAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 2월 14일, 21:17 UTC
- 편집된 시간: 2018년 11월 14일, 00:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy는 AWS 관리형 정책으로, AWS Ground Station Agent를 사용할 수 있는 Dataflow Endpoint Instance 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSGroundStationAgentInstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 29일, 15:23 UTC
- 편집된 시간: 2023년 3월 29일, 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSHealth_EventProcessorServiceRolePolicy

`AWSHealth_EventProcessorServiceRolePolicy`는 AWS 관리형 정책으로, AWS Health가 Health 이벤트 프로세서 기능을 활성화할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 13일, 19:24 UTC
- 편집된 시간: 2023년 1월 13일, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSHealthFullAccess

`AWSHealthFullAccess`는 AWS 관리형 정책으로, AWS Health API 및 Notifications와 Personal Health Dashboard에 대한 전체 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSHealthFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 6일, 12:30 UTC
- 편집된 시간: 2020년 11월 16일, 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSHealthImagingFullAccess

`AWSHealthImagingFullAccess`는 AWS 관리형 정책으로, AWS Health Imaging 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSHealthImagingFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2023년 7월 25일, 23:39 UTC
- 편집된 시간: 2023년 7월 25일, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess는 AWS 관리형 정책으로, AWS Health Imaging 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSHealthImagingReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 7월 25일, 23:40 UTC
- 편집된 시간: 2023년 8월 1일, 15:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIAMIdentityCenterAllowListForIdentityContext

`AWSIAMIdentityCenterAllowListForIdentityContext`는 AWS 관리형 정책으로, IAM Identity Center 자격 증명 컨텍스트에서 맡은 역할에 허용되는 작업 목록을 제공합니다. AWS Security Token Service(AWSSTS)는 이 정책을 위임된 역할에 자동으로 연결합니다. 아이덴티티 컨텍스트는 로 ProvidedContext 전달됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIAMIdentityCenterAllowListForIdentityContext`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 8일, 15:21 UTC
- 편집 시간: 2023년 11월 25일 19:27 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
```

```
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIdentitySyncFullAccess

`AWSIdentitySyncFullAccess`는 AWS 관리형 정책으로, Identity Sync 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIdentitySyncFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 3월 23일, 23:29 UTC
- 편집된 시간: 2022년 3월 23일, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIdentitySyncReadOnlyAccess

`AWSIdentitySyncReadOnlyAccess`는 AWS 관리형 정책으로, Identity Sync 서비스에 대한 읽기 전용 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIdentitySyncReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 3월 23일, 23:29 UTC
- 편집된 시간: 2022년 3월 23일, 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSImageBuilderFullAccess

AWSImageBuilderFullAccess는 AWS 관리형 정책으로, 모든 AWS Image Builder 작업에 대한 전체 액세스 권한과 관련 AWS 서비스에 대한 리소스 범위 지정 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSImageBuilderFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 20일, 18:25 UTC
- 편집된 시간: 2021년 4월 13일, 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSImageBuilderReadOnlyAccess

`AWSImageBuilderReadOnlyAccess`는 AWS 관리형 정책으로, 모든 AWS Image Builder 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSImageBuilderReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 19일, 22:29 UTC
- 편집된 시간: 2019년 12월 19일, 22:29 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSImportExportFullAccess

AWSImportExportFullAccess는 AWS 관리형 정책으로, AWS 계정에 생성된 작업에 대한 읽기 및 쓰기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSImportExportFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSImportExportReadOnlyAccess

`AWSImportExportReadOnlyAccess`는 AWS 관리형 정책으로, AWS 계정에 생성된 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSImportExportReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIncidentManagerIncidentAccessServiceRolePolicy

`AWSIncidentManagerIncidentAccessServiceRolePolicy`인시던트 관리의 일환으로 인시던트 AWS 관리자에게 다른 AWS 서비스를 호출할 수 있는 권한을 부여하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIncidentManagerIncidentAccessServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 13일, 00:01 UTC
- 편집 시간: 2024년 2월 20일 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSIncidentManagerResolverAccess

AWSIncidentManagerResolverAccess는 AWS 관리형 정책으로, 이 정책은 사용자 지정 타임라인 이벤트 및 관련 항목에 대한 전체 액세스 권한과 함께 인시던트를 시작, 조회 및 업데이트할 수 있는 권한을 부여합니다. 인시던트를 생성하고 해결할 사용자에게 이 정책을 할당하세요.

이 정책 사용

사용자, 그룹 및 역할에 AWSIncidentManagerResolverAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 5월 10일, 06:12 UTC
- 편집된 시간: 2021년 5월 10일, 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIncidentManagerServiceRolePolicy

`AWSIncidentManagerServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 인시던트 관리자에게 사용자를 대신하여 인시던트 기록 및 관련 리소스를 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 10일, 03:34 UTC
- 편집된 시간: 2022년 12월 5일, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess는 AWS 관리형 정책으로, AWS IoT 1-Click에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoT1ClickFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 11일, 22:10 UTC
- 편집된 시간: 2018년 5월 11일, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess는 AWS 관리형 정책으로, AWS IoT 1-Click에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoT1ClickReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 11일, 21:49 UTC
- 편집된 시간: 2018년 5월 11일, 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTAnalyticsFullAccess

`AWSIoTAnalyticsFullAccess`는 AWS 관리형 정책으로, IoT Analytics에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTAnalyticsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 18일, 23:02 UTC
- 편집된 시간: 2018년 6월 18일, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTAnalyticsReadOnlyAccess

`AWSIoTAnalyticsReadOnlyAccess`는 AWS 관리형 정책으로, IoT Analytics에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTAnalyticsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 18일, 21:37 UTC
- 편집된 시간: 2018년 6월 18일, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTConfigAccess

`AWSIoTConfigAccess`는 AWS 관리형 정책으로, 이 정책은 AWS IoT 구성 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTConfigAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:52 UTC
- 편집된 시간: 2019년 9월 27일, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTConfigReadOnlyAccess

`AWSIoTConfigReadOnlyAccess`는 AWS 관리형 정책으로, 이 정책은 AWS IoT 구성 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTConfigReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:52 UTC
- 편집된 시간: 2019년 9월 27일, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDataAccess

`AWSIoTDataAccess`는 AWS 관리형 정책으로, 이 정책은 AWS IoT 메시징 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDataAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 27일, 21:51 UTC
- 편집된 시간: 2021년 6월 23일, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`는 AWS 관리형 정책으로, ADD_THINGS_TO_THING_GROUP 완화 조치 실행을 위해 IoT 사물 그룹에 대한 쓰기 액세스와 IoT 인증서에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2019년 8월 7일, 17:55 UTC
- 편집된 시간: 2019년 8월 7일, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderAudit

AWSIoTDeviceDefenderAudit는 AWS 관리형 정책으로, IoT 및 관련 리소스에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderAudit를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 7월 18일, 21:17 UTC
- 편집된 시간: 2019년 11월 25일, 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`는 AWS 관리형 정책으로, ENABLE_IOT_LOGGING 완화 조치 실행을 위해 IoT 로깅을 활성화하기 위한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction는 AWS 관리형 정책으로, PUBLISH_FINDING_TO_SNS 완화 조치 실행을 위해 SNS 주제에 대한 메시지 게시 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`는 AWS 관리형 정책으로, REPLACE_DEFAULT_POLICY_VERSION 완화 조치 실행을 위해 IoT 정책에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:04 UTC
- 편집된 시간: 2019년 8월 7일, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction는 AWS 관리형 정책으로, UPDATE_CA_CERTIFICE 완화 조치 실행을 위해 IoT CA 인증서에 대한 쓰기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderUpdateCACertMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:05 UTC
- 편집된 시간: 2019년 8월 7일, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction는 AWS 관리형 정책으로, UPDATE_DEVICE_CERTIFICATE 완화 조치 실행을 위해 IoT 인증서에 대한 쓰기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 8월 7일, 17:06 UTC
- 편집된 시간: 2019년 8월 7일, 17:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceTesterForFreeRTOSFullAccess

`AWSIoTDeviceTesterForFreeRTOSFullAccess`는 AWS 관리형 정책으로, AWS IoT Device Tester가 IoT, S3 및 IAM을 포함한 서비스에 대한 액세스를 허용하여 FreeRTOS 검증 제품군을 실행할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceTesterForFreeRTOSFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 12일, 20:33 UTC
- 편집된 시간: 2023년 8월 10일, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTDeviceTesterForGreengrassFullAccess

`AWSIoTDeviceTesterForGreengrassFullAccess`는 AWS 관리형 정책으로, AWS IoT Device Tester가 Lambda, IoT, API Gateway, IAM을 포함한 관련 서비스에 대한 액세스를 허용하여 AWS Greengrass 검증 제품군을 실행할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTDeviceTesterForGreengrassFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 2월 20일, 21:21 UTC
- 편집된 시간: 2020년 6월 25일, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTEventsFullAccess

`AWSIoTEventsFullAccess`는 AWS 관리형 정책으로, IoT Events에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTEventsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 10일, 22:51 UTC
- 편집된 시간: 2019년 1월 10일, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTEventsReadOnlyAccess

`AWSIoTEventsReadOnlyAccess`는 AWS 관리형 정책으로, IoT Events에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTEventsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 10일, 22:50 UTC

- 편집된 시간: 2019년 9월 23일, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTFleetHubFederationAccess

`AWSIoTFleetHubFederationAccess`는 AWS 관리형 정책으로, IoT Fleet Hub 애플리케이션에 대한 페더레이션 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTFleetHubFederationAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 15일, 08:08 UTC
- 편집된 시간: 2022년 4월 4일, 18:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTFleetwiseServiceRolePolicy

`AWSIoTFleetwiseServiceRolePolicy`는 AWS 관리형 정책으로, 보조 기능을 위해 AWSIoTFleetwise에서 사용하거나 관리하는 AWS 리소스 및 메타데이터에 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 9월 21일, 23:27 UTC
- 편집된 시간: 2022년 9월 21일, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTFullAccess

`AWSIoTFullAccess`는 AWS 관리형 정책으로, 이 정책은 AWS IoT 구성 및 메시징 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 8일, 15:19 UTC
- 편집된 시간: 2022년 5월 19일, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTLogging

AWSIoTLogging는 AWS 관리형 정책으로, Amazon CloudWatch Log 그룹을 생성하고 로그를 그룹으로 스트리밍할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTLogging를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 10월 8일, 15:17 UTC
- 편집된 시간: 2015년 10월 8일, 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTOTAUpdate

AWSIoTOTAUpdate는 AWS 관리형 정책으로, AWS IoT Job을 생성하고 AWS 코드 서명자 작업을 설명하기 위한 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTOTAUpdate를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 12월 20일, 20:36 UTC
- 편집된 시간: 2017년 12월 20일, 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIotRoboRunnerFullAccess

AWSIotRoboRunnerFullAccess는 AWS 관리형 정책으로, 이 정책은 AWS Iot RoborUnner에 대한 전체 액세스를 허용하는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIotRoboRunnerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 03:54 UTC
- 편집된 시간: 2023년 2월 23일, 18:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIotRoboRunnerReadOnly

AWSIotRoboRunnerReadOnly는 AWS 관리형 정책으로, 이 정책은 AWS Iot RoborUnner에 대한 읽기 전용 액세스를 허용하는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIotRoboRunnerReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 03:43 UTC
- 편집된 시간: 2022년 11월 16일, 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIotRoboRunnerServiceRolePolicy

AWSIotRoboRunnerServiceRolePolicy는 AWS 관리형 정책으로, AWS IoT RoboRunner가 고객을 대신하여 연관된 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 2월 21일, 16:56 UTC
- 편집된 시간: 2023년 2월 21일, 16:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTRuleActions

AWSIoTRuleActions는 AWS 관리형 정책으로, AWS IoT Rule Actions에서 지원되는 모든 AWS 서비스에 대한 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTRuleActions를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 10월 8일, 15:14 UTC
- 편집된 시간: 2018년 1월 16일, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTSiteWiseConsoleFullAccess

`AWSIoTSiteWiseConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 사용하여 AWS IoT SiteWise를 관리할 수 있는 전체 액세스를 제공합니다. 이 정책은 또한 AWS IoT SiteWise(예: AWS IoT Analytics)와 함께 사용되는 데이터 스토어를 생성 및 나열할 수 있는 액세스, AWS IoT Greengrass 리소스 나열 및 보기, AWS Secrets Manager 비밀 나열 및 수정, AWS IoT 사물 섀도우 검색, 특정 태그가 있는 리소스 나열, AWS IoT SiteWise에 대한 서비스 연결 역할 생성 및 사용에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTSiteWiseConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 5월 31일, 21:37 UTC
- 편집된 시간: 2019년 5월 31일, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTSiteWiseFullAccess

AWSIoTSiteWiseFullAccess는 AWS 관리형 정책으로, IoT SiteWise에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTSiteWiseFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 4일, 20:53 UTC
- 편집된 시간: 2018년 12월 4일, 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTSiteWiseMonitorPortalAccess

`AWSIoTSiteWiseMonitorPortalAccess`는 AWS 관리형 정책으로, 이 정책은 AWS IoT SiteWise 자산 및 자산 데이터에 액세스하고, AWS IoT SiteWise Monitor 리소스를 생성하고, AWS SSO 사용자를 나열할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTSiteWiseMonitorPortalAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 5월 19일, 20:01 UTC
- 편집된 시간: 2020년 5월 19일, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTSiteWiseMonitorServiceRolePolicy

`AWSIoTSiteWiseMonitorServiceRolePolicy`는 AWS 관리형 정책으로, AWS IoT SiteWise 자산 및 자산 자산에 액세스하고, AWS IoT SiteWise 포털을 통해 AWS IoT Sitewise 프로젝트, 대시보드 및 액세스 정책을 생성할 수 있는 AWS IoT SiteWise 모니터 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 14일, 00:59 UTC
- 편집된 시간: 2019년 12월 13일, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTSiteWiseReadOnlyAccess

AWSIoTSiteWiseReadOnlyAccess는 AWS 관리형 정책으로, IoT SiteWise에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTSiteWiseReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 12월 4일, 20:55 UTC
- 편집된 시간: 2022년 9월 16일, 19:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTThingsRegistration

`AWSIoTThingsRegistration`는 AWS 관리형 정책으로, 이 정책은 사용자가 AWS IoT StartThingRegistrationTask API를 사용하여 대량으로 사물을 등록할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTThingsRegistration`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 12월 1일, 20:21 UTC
- 편집된 시간: 2020년 10월 5일, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTTwinMakerServiceRolePolicy

`AWSIoTTwinMakerServiceRolePolicy`AWS TwinMaker IoT가 사용자 대신 다른 AWS 서비스를 호출하고 리소스를 동기화할 수 있도록 허용하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 13일, 18:59 UTC
- 편집된 시간: 2023년 11월 13일, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessDataAccess

`AWSIoTWirelessDataAccess`는 AWS 관리형 정책으로, AWS IoT Wireless 디바이스에 연관된 자격 증명 데이터 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessDataAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:31 UTC
- 편집된 시간: 2020년 12월 15일, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessFullAccess

`AWSIoTWirelessFullAccess`는 AWS 관리형 정책으로, 모든 AWS IoT Wireless 작업에 대한 연관된 자격 증명 전체 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:27 UTC
- 편집된 시간: 2020년 12월 15일, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessFullPublishAccess

AWSIoTWirelessFullPublishAccess는 AWS 관리형 정책으로, 사용자를 대신하여 IoT Rules Engine에 게시할 수 있는 IoT Wireless 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIoTWirelessFullPublishAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:29 UTC
- 편집된 시간: 2020년 12월 15일, 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessGatewayCertManager

`AWSIoTWirelessGatewayCertManager`는 AWS 관리형 정책으로, 연관된 자격 증명으로 IoT 인증서를 생성, 나열 및 설명할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessGatewayCertManager`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:30 UTC
- 편집된 시간: 2020년 12월 15일, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessLogging

`AWSIoTWirelessLogging`는 AWS 관리형 정책으로, 연관된 자격 증명이 Amazon CloudWatch Logs 그룹을 생성하고 로그를 그룹에 스트리밍하도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessLogging`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:32 UTC
- 편집된 시간: 2020년 12월 15일, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIoTWirelessReadOnlyAccess

`AWSIoTWirelessReadOnlyAccess`는 AWS 관리형 정책으로, AWS IoT 무선에 연관된 자격 증명 읽기 전용 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSIoTWirelessReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 15일, 15:28 UTC
- 편집된 시간: 2020년 12월 15일, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIPAMServiceRolePolicy

AWSIPAMServiceRolePolicy는 AWS 관리형 정책으로, VPC IP 주소 관리자가 사용자를 대신하여 VPC 리소스에 액세스하고 AWS Organizations와 통합할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 30일, 19:08 UTC
- 편집된 시간: 2023년 11월 8일, 19:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy는 AWS 관리형 정책으로, 고객을 대신하여 AWS IQ에서 결제 요청을 실행하는 데 사용됩니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 22일, 19:28 UTC
- 편집된 시간: 2019년 8월 22일, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIQFullAccess

AWSIQFullAccess는 AWS 관리형 정책으로, AWS IQ에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSIQFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 4월 4일, 23:13 UTC
- 편집된 시간: 2019년 9월 25일, 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSIQPermissionServiceRolePolicy

`AWSIQPermissionServiceRolePolicy`는 AWS 관리형 정책으로, AWS IQ가 AWS IQ 전문가가 맡는 역할을 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 22일, 19:36 UTC
- 편집된 시간: 2019년 8월 22일, 19:36 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`는 AWS 관리형 정책으로, AWS KMS 사용자 지정 키 스토어에 필요한 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 20:10 UTC
- 편집된 시간: 2023년 11월 10일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy는 AWS 관리형 정책으로, AWS KMS가 다중 리전 키의 공유 속성을 동기화할 수 있도록 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 16일, 15:37 UTC

- 편집된 시간: 2021년 6월 16일, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSKeyManagementServicePowerUser

`AWSKeyManagementServicePowerUser`는 AWS 관리형 정책으로, AWS Key Management Service(KMS)에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSKeyManagementServicePowerUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2017년 3월 7일, 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLakeFormationCrossAccountManager

`AWSLakeFormationCrossAccountManager`는 AWS 관리형 정책으로, Lake Formation을 통해 Glue 리소스에 대한 교차 계정 액세스를 제공합니다. 또한 조직 및 리소스 액세스 관리자와 같은 기타 필수 서비스에 대한 읽기 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLakeFormationCrossAccountManager`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 4일, 20:59 UTC
- 편집된 시간: 2023년 11월 1일, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin는 AWS 관리형 정책으로, 데이터 레이크를 관리하기 위해 AWS Lake Formation 및 관련 서비스(예: AWS Glue)에 대한 관리자 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLakeFormationDataAdmin를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 8월 8일, 17:33 UTC
- 편집된 시간: 2019년 12월 16일, 22:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
```

```
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:GetWorkflow",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambda_FullAccess

AWSLambda_FullAccess는 AWS 관리형 정책으로, AWS Lambda 서비스, AWS Lambda 콘솔 기능 및 기타 관련 AWS 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambda_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 17일, 21:14 UTC
- 편집된 시간: 2020년 11월 17일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambda_ReadOnlyAccess

`AWSLambda_ReadOnlyAccess`는 AWS 관리형 정책으로, AWS Lambda 서비스, AWS Lambda 콘솔 기능 및 기타 관련 AWS 서비스에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambda_ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 17일, 21:10 UTC
- 편집된 시간: 2023년 7월 27일, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaBasicExecutionRole

`AWSLambdaBasicExecutionRole`는 AWS 관리형 정책으로, CloudWatch Logs에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambdaBasicExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:03 UTC
- 편집된 시간: 2015년 4월 9일, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaDynamoDBExecutionRole

`AWSLambdaDynamoDBExecutionRole`는 AWS 관리형 정책으로, DynamoDB 스트림에 대한 목록 및 읽기 액세스와 CloudWatch 로그에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambdaDynamoDBExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:09 UTC
- 편집된 시간: 2015년 4월 9일, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess는 AWS 관리형 정책으로, Lambda 함수가 VPC 지원 Lambda 함수에서 사용하는 ENI를 관리(생성, 설명, 삭제)하기 위해 Lambda 함수에 대한 최소 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaENIManagementAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 6일, 00:37 UTC
- 편집된 시간: 2020년 10월 1일, 20:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaExecute

AWSLambdaExecute는 AWS 관리형 정책으로, S3에 대한 Put, Get 액세스와 CloudWatch Logs에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaExecute를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaFullAccess

AWSLambdaFullAccess는 AWS 관리형 정책으로, 이 정책은 사용 중단 중입니다. 지침은 설명서를 참조하세요. https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html Lambda, S3, DynamoDB, CloudWatch 지표 및 로그에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2017년 11월 27일, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaInvocation-DynamoDB

`AWSLambdaInvocation-DynamoDB`는 AWS 관리형 정책으로, DynamoDB 스트림에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambdaInvocation-DynamoDB`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2015년 2월 6일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaKinesisExecutionRole

`AWSLambdaKinesisExecutionRole`는 AWS 관리형 정책으로, Kinesis 스트림에 대한 목록 및 읽기 액세스와 CloudWatch 로그에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambdaKinesisExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 4월 9일, 15:14 UTC

- 편집된 시간: 2018년 11월 19일, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaMSKExecutionRole

AWSLambdaMSKExecutionRole는 AWS 관리형 정책으로, VPC 내의 MSK Cluster에 액세스하고, VPC에서 ENI를 관리(생성, 설명, 삭제)하는 데 필요한 권한 및 CloudWatch Logs에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaMSKExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 11일, 17:35 UTC
- 편집된 시간: 2022년 8월 2일, 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaReplicator

`AWSLambdaReplicator`는 AWS 관리형 정책으로, Lambda Replicator에 리전 간 함수를 복제하는 데 필요한 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 5월 23일, 17:53 UTC
- 편집된 시간: 2017년 12월 8일, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaRole

AWSLambdaRole은 AWS 관리형 정책으로, AWS Lambda 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaSQSQueueExecutionRole

`AWSLambdaSQSQueueExecutionRole`는 AWS 관리형 정책으로, SQS 대기열에 대한 메시지 수신, 메시지 삭제, 속성 읽기 액세스와 CloudWatch 로그에 대한 쓰기 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLambdaSQSQueueExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 6월 14일, 21:50 UTC

- 편집된 시간: 2018년 6월 14일, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole는 VPC 내에서 리소스에 액세스하는 동안 Lambda 함수를 실행할 수 있는 최소 권한 (네트워크 인터페이스를 생성, 설명, 삭제하고 로그에 대한 쓰기 권한) 을 제공하는 AWS관리형 정책입니다. CloudWatch

이 정책 사용

사용자, 그룹 및 역할에 AWSLambdaVPCAccessExecutionRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 2월 11일, 23:15 UTC
- 편집 시간: 2024년 1월 5일 22:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerConsumptionPolicy

`AWSLicenseManagerConsumptionPolicy`는 AWS 관리형 정책으로, 사용자에게 자격이 있는 AWS 라이선스를 사용하는 데 필요한 License Manager API 작업에 대한 액세스를 허용하는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSLicenseManagerConsumptionPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 8월 11일, 23:18 UTC
- 편집된 시간: 2021년 8월 11일, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`는 AWS 관리형 정책으로, AWS License Manager Linux 구독 서비스가 사용자를 대신하여 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 12월 20일, 18:54 UTC
- 편집된 시간: 2022년 12월 20일, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy는 AWS 관리형 정책으로, AWS License Manager 서비스 마스터 계정 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:03 UTC
- 편집된 시간: 2022년 5월 31일, 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerMemberAccountRolePolicy

AWSLicenseManagerMemberAccountRolePolicy는 AWS 관리형 정책으로, AWS License Manager 서비스 멤버 계정 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:04 UTC
- 편집된 시간: 2019년 11월 15일, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy는 AWS 관리형 정책으로, AWS License Manager 서비스 기본 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 19:02 UTC
- 편집된 시간: 2021년 7월 30일, 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy는 AWS 관리형 정책으로, AWS License Manager User 구독 서비스가 사용자를 대신하여 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 30일, 01:17 UTC
- 편집된 시간: 2022년 11월 21일, 19:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
```

```
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSM2ServicePolicy

AWSM2ServicePolicy는 AWS 관리형 정책으로, AWS M2가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 7일, 20:26 UTC
- 편집된 시간: 2022년 6월 7일, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSManagedServices_ContactsServiceRolePolicy

`AWSManagedServices_ContactsServiceRolePolicy`는 AWS 관리형 정책으로, AWS Managed Services가 AWS 리소스의 태그 값을 읽을 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 23일, 17:07 UTC
- 편집된 시간: 2023년 3월 23일, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`는 AWS 관리형 정책으로, AWS Managed Services - 탐지 제어 인프라를 관리하기 위한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 12월 19일, 23:11 UTC
- 편집된 시간: 2022년 12월 19일, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSManagedServices_EventsServiceRolePolicy

`AWSManagedServices_EventsServiceRolePolicy`는 AWS 관리형 정책으로, AMS 이벤트 프로세서 기능을 활성화하기 위한 AWS Managed Services 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 2월 7일, 18:41 UTC
- 편집된 시간: 2023년 2월 7일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSManagedServicesDeploymentToolkitPolicy

AWSManagedServicesDeploymentToolkitPolicy는 AWS 관리형 정책으로, AWS Managed Services가 사용자를 대신하여 배포 툴킷을 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 9일, 18:33 UTC
- 편집된 시간: 2023년 5월 10일, 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
```

```
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion은 AWS 관리형 정책으로, AWS Marketplace이 Amazon Machine Image(AMI)를 복사하여 AWS Marketplace에 나열할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceAmiIngestion를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 25일, 20:55 UTC
- 편집된 시간: 2020년 9월 25일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceDeploymentServiceRolePolicy

`AWSMarketplaceDeploymentServiceRolePolicy`는 AWS 관리형 정책으로, AWS Marketplace이 AWS Marketplace에서 구독하는 제품에 대한 판매자 배포 파라미터를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2023년 11월 15일, 23:34 UTC
- 편집된 시간: 2023년 11월 15일, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceFullAccess

AWSMarketplaceFullAccess는 AWS 관리형 정책으로, AWS Marketplace 소프트웨어를 구독하거나 구독 해지할 수 있는 권한을 부여하고, 사용자에게 Marketplace '사용자 소프트웨어' 페이지에서 Marketplace 소프트웨어 인스턴스를 관리할 수 있도록 허용하고, EC2에 대한 관리자 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 11일, 17:21 UTC
- 편집된 시간: 2022년 3월 4일, 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish",
        "sns:setTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:*image-build*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceGetEntitlements

`AWSMarketplaceGetEntitlements`는 AWS 관리형 정책으로, AWS Marketplace Entitlements에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceGetEntitlements를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 3월 27일, 19:37 UTC
- 편집된 시간: 2017년 3월 27일, 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess는 AWS 관리형 정책으로, AWS Marketplace Private Image Build Feature에 대한 전체 액세스를 제공합니다. 프라이빗 이미지를 생성하는 것 외에도 이미지에 태그를 추가하고, ec2 인스턴스를 시작 및 종료할 수 있는 권한도 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceImageBuildFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 7월 31일, 23:29 UTC
- 편집된 시간: 2022년 3월 4일, 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceLicenseManagementServiceRolePolicy

`AWSMarketplaceLicenseManagementServiceRolePolicy`는 AWS 관리형 정책으로, 라이선스 관리를 위해 AWS Marketplace에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 3일, 08:33 UTC
- 편집된 시간: 2020년 12월 3일, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`는 AWS 관리형 정책으로, AWS Marketplace 소프트웨어 구독 및 구독 취소 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceManageSubscriptions를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 1월 19일, 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceMeteringFullAccess

`AWSMarketplaceMeteringFullAccess`는 AWS 관리형 정책으로, AWS Marketplace 측정에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMarketplaceMeteringFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 3월 17일, 22:39 UTC
- 편집된 시간: 2016년 3월 17일, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceMeteringRegisterUsage

`AWSMarketplaceMeteringRegisterUsage`는 AWS 관리형 정책으로, AWS Marketplace 측정 서비스를 통해 리소스를 등록하고 사용량을 추적할 수 있는 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMarketplaceMeteringRegisterUsage`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 11월 21일, 01:17 UTC
- 편집된 시간: 2019년 11월 21일, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceProcurementSystemAdminFullAccess

`AWSMarketplaceProcurementSystemAdminFullAccess`는 AWS 관리형 정책으로, AWS Marketplace eProcurement 통합을 위한 모든 관리 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceProcurementSystemAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 25일, 13:07 UTC
- 편집된 시간: 2019년 6월 25일, 13:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplacePurchaseOrdersServiceRolePolicy

`AWSMarketplacePurchaseOrdersServiceRolePolicy`는 AWS 관리형 정책으로, 구매 주문 관리 위해 AWS Marketplace 서비스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 27일, 15:12 UTC
- 편집된 시간: 2021년 10월 27일, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceRead-only

`AWSMarketplaceRead-only`는 AWS 관리형 정책으로, AWS Marketplace 구독을 검토하는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMarketplaceRead-only`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2023년 1월 19일, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow"
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:DescribeBuilds",
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ]
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceResaleAuthorizationServiceRolePolicy

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`재판매 승인을 위해 AWS 서비스 사용하거나 AWS 관리하는 리소스에 AWS Marketplace 대한 액세스를 가능하게 하는 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2024년 3월 5일 18:47 UTC
- 편집 시간: 2024년 3월 5일 18:47 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSMarketplaceSellerFullAccess

`AWSMarketplaceSellerFullAccess`는 AMI 관리와 같은 기타 AWS 서비스에 대한 모든 셀러 작업에 대한 전체 액세스 권한을 제공하는 AWS 관리형 정책입니다. AWS Marketplace

이 정책 사용

사용자, 그룹 및 역할에 `AWSMarketplaceSellerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2019년 7월 2일, 20:40 UTC
- 편집 시간: 2024년 3월 15일 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewMarketing",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace-management:viewSettings",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "aws-marketplace:GetSellerDashboard",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSMarketplaceSellerProductsFullAccess

AWSMarketplaceSellerProductsFullAccess는 AWS 관리형 정책으로, 판매자에게 AWS Marketplace 관리 제품 페이지 및 AMI 관리와 같은 기타 AWS 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMarketplaceSellerProductsFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 2일, 21:06 UTC
- 편집된 시간: 2023년 7월 18일, 22:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
```

```
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMarketplaceSellerProductsReadOnly

`AWSMarketplaceSellerProductsReadOnly`는 AWS 관리형 정책으로, 판매자에게 AWS Marketplace 관리 제품 페이지에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMarketplaceSellerProductsReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 2일, 21:40 UTC

- 편집된 시간: 2022년 11월 19일, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy는 AWS 관리형 정책으로, MediaConnect에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화하는 기본 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 3일, 22:11 UTC
- 편집된 시간: 2023년 4월 3일, 22:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy는 AWS 관리형 정책으로, MediaTailor에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 17일, 22:27 UTC
- 편집된 시간: 2021년 9월 17일, 22:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubDiscoveryAccess

AWSMigrationHubDiscoveryAccess는 AWS 관리형 정책으로, AWSMigrationHubService가 고객을 대신하여 AWSApplicationDiscoveryService를 호출하도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubDiscoveryAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:30 UTC
- 편집된 시간: 2020년 8월 6일, 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubDMSAccess

`AWSMigrationHubDMSAccess`는 AWS 관리형 정책으로, Database Migration Service가 고객의 계정에서 역할을 맡아 Migration Hub를 호출하도록 하기 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMigrationHubDMSAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 14:00 UTC
- 편집된 시간: 2019년 10월 7일, 17:51 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubFullAccess

`AWSMigrationHubFullAccess`는 AWS 관리형 정책으로, 고객에게 Migration Hub 서비스에 대한 액세스를 제공하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMigrationHubFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 8월 14일, 14:02 UTC
- 편집된 시간: 2019년 6월 19일, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubOrchestratorConsoleFullAccess

`AWSMigrationHubOrchestratorConsoleFullAccess`는 AWS 관리형 정책으로, AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service 및 AWS Secrets Manager에 대한 제한된 액세스를 제공합니다. 이 정책은 또한 AWS Migration Hub Orchestrator 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMigrationHubOrchestratorConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 20일, 02:26 UTC
- 편집 시간: 2023년 12월 5일 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy는 AWS 관리형 정책으로, 이 정책은 당사 서비스가 S3에서 스크립트를 다운로드하여 인스턴스를 오케스트레이션하고 EC2 인스턴스 내에서 비밀 값을 가져오도록 SAP 및 MGN 마이그레이션 인스턴스에 연결되어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubOrchestratorInstanceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 4월 20일, 02:43 UTC
- 편집된 시간: 2022년 4월 20일, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubOrchestratorPlugin

`AWSMigrationHubOrchestratorPlugin`은 AWS 관리형 정책으로, AWS Migration Hub Orchestrator의 Amazon Simple Storage Service, AWS Secrets Manager 및 플러그인 관련 작업에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMigrationHubOrchestratorPlugin`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 20일, 02:25 UTC
- 편집된 시간: 2022년 4월 20일, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubOrchestratorServiceRolePolicy

`AWSMigrationHubOrchestratorServiceRolePolicy`는 AWS 관리형 정책으로, Migration Hub Orchestrator가 온프레미스 워크로드를 마이그레이션하고 현대화하는 데 필요한 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 4월 20일, 02:24 UTC
- 편집 시간: 2024년 3월 4일 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess는 AWS 관리형 정책으로, 네트워크 브리지가 없는 환경을 사용할 때는 필요하지 않은 AWS Transit Gateway 및 EC2 보안 그룹을 제외한 AWS Migration Hub Refactor Spaces 및 기타 AWS 관련 서비스에 대한 전체 액세스를 부여합니다. 또한 이 정책은 태그를 기준으로 범위를 축소할 수 있는 AWS Lambda 및 AWS Resource Access Manager에 필요한 권한을 제외합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 4월 3일, 20:09 UTC
- 편집된 시간: 2023년 7월 20일, 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
```

```
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`는 AWS 관리형 정책으로, SSM 자동화 문서 AWSRefactorSpaces-CreateResources에 전달된 IAM 서비스 역할에서 사용하여 자동화를 실행하는 데 필요한 권한을 부여합니다. 이 정책은 자동화 진행 상황을 추적하기 위해 EC2 태그에 대한 읽기/쓰기 액세스를 부여합니다. 또한 Refactor Spaces 환경의 네트워크 브리지가 활성화되면 자동화는 환경의 보안 그룹을 EC2 인스턴스에 추가하여 환경의 다른 Refactor Spaces 서비스로부터의 트래픽을 허용합니다. 또한 이 정책은Application Migration Service의 시작 후 작업 SSM 파라미터에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2023년 8월 10일, 15:08 UTC
- 편집된 시간: 2023년 8월 10일, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubRefactorSpacesFullAccess

`AWSMigrationHubRefactorSpacesFullAccess`는 AWS 관리형 정책으로, 태그를 기반으로 범위를 좁힐 수 있으므로 태그를 기준으로 범위를 축소할 수 있는 AWS Lambda 및 AWS Resource

Access Manager에 필요한 권한을 제외하고 AWS MigrationHub Refactor Spaces, AWS MigrationHub Refactor Spaces 콘솔 기능 및 기타 관련 AWS 서비스에 대한 전체 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubRefactorSpacesFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 11월 29일, 07:12 UTC
- 편집된 시간: 2023년 7월 19일, 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
```

```
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
```

```
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubRefactorSpacesServiceRolePolicy

`AWSMigrationHubRefactorSpacesServiceRolePolicy`는 AWS 관리형 정책으로, AWS Migration Hub Refactor Spaces에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 29일, 06:50 UTC
- 편집된 시간: 2023년 7월 20일, 15:57 UTC

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

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess는 AWS 관리형 정책으로, Server Migration Service가 고객의 계정에서 역할을 맡아 Migration Hub를 호출하도록 하기 위한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubSMSAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 8월 14일, 13:57 UTC
- 편집된 시간: 2019년 10월 7일, 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubStrategyCollector

AWSMigrationHubStrategyCollector는 AWS 관리형 정책으로, AWS Migration Hub Strategy Recommendations 서비스와의 통신, 서비스와 관련된 S3 버킷에 대한 읽기/쓰기 액세스, 로그 및 지표를 AWS에 업로드하기 위한 Amazon API Gateway 액세스, 자격 증명을 가져오기 위한 AWS Secrets Manager 액세스 및 기타 관련 서비스를 허용할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubStrategyCollector를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 19일, 20:15 UTC
- 편집 시간: 2024년 2월 5일 18:57 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
```

```
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
```

```
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubStrategyConsoleFullAccess

AWSMigrationHubStrategyConsoleFullAccess는 AWS 관리형 정책으로, AWS Migration Hub Strategy Recommendations 서비스에 대한 전체 액세스와 AWS Management Console을 통해 관련 AWS 서비스에 대한 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMigrationHubStrategyConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 10월 19일, 20:13 UTC
- 편집된 시간: 2022년 11월 9일, 00:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMigrationHubStrategyServiceRolePolicy

AWSMigrationHubStrategyServiceRolePolicy는 AWS 관리형 정책으로, AWS Migration Hub Strategy Recommendations에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 19일, 20:02 UTC
- 편집된 시간: 2021년 10월 19일, 20:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMobileHub_FullAccess

AWSMobileHub_FullAccess는 AWS 관리형 정책으로, 이 정책은 사용자에게 AWS Mobile Hub에서 프로젝트(및 해당 연관된 AWS 리소스)를 생성, 삭제 및 수정할 수 있는 권한을 부여하기 위해 모든 사용자, 역할 또는 그룹에 연결할 수 있습니다. 여기에는 각 Mobile Hub 프로젝트에 대한 샘플 모바일 앱 소스 코드를 생성하고 다운로드할 수 있는 권한도 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMobileHub_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 5일, 19:56 UTC
- 편집된 시간: 2019년 12월 19일, 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMobileHub_ReadOnly

AWSMobileHub_ReadOnly는 AWS 관리형 정책으로, 이 정책은 사용자에게 AWS Mobile Hub에서 프로젝트를 나열하고 볼 수 있는 권한을 부여하기 위해 모든 사용자, 역할 또는 그룹에 연결할 수 있습니다. 여기에는 각 Mobile Hub 프로젝트에 대한 샘플 모바일 앱 소스 코드를 생성하고 다운로드할 수 있는 권한도 포함됩니다. 사용자는 Mobile Hub 프로젝트에 대한 구성을 수정할 수 없습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSMobileHub_ReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 1월 5일, 19:55 UTC
- 편집된 시간: 2018년 7월 23일, 21:59 UTC

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

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSMSKReplicatorExecutionRole

`AWSMSKReplicatorExecutionRole`는 다음과 같은 AWS관리형 정책입니다. Amazon MSK Replicator에 MSK 클러스터 간에 데이터를 복제할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSMSKReplicatorExecutionRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 12월 6일 00:07 UTC
- 편집 시간: 2023년 12월 6일 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
```

```
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSNetworkFirewallServiceRolePolicy

`AWSNetworkFirewallServiceRolePolicy`는 AWS 관리형 정책으로, AWSNetworkFirewall이 방화벽에 필요한 리소스를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 17일, 17:17 UTC
- 편집된 시간: 2023년 3월 30일, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy는 AWS 관리형 정책으로, NetworkManager가 코어 네트워크와 연관된 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 12일, 12:17 UTC
- 편집된 시간: 2022년 7월 12일, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSNetworkManagerFullAccess

`AWSNetworkManagerFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon NetworkManager에 대한 전체 액세스를 제공하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSNetworkManagerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 17:37 UTC
- 편집된 시간: 2019년 12월 3일, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSNetworkManagerReadOnlyAccess

AWSNetworkManagerReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon NetworkManager에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSNetworkManagerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 3일, 17:35 UTC
- 편집된 시간: 2019년 12월 3일, 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSNetworkManagerServiceRolePolicy

`AWSNetworkManagerServiceRolePolicy`는 AWS 관리형 정책으로, NetworkManager가 글로벌 네트워크와 연관된 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 3일, 14:03 UTC
- 편집된 시간: 2022년 7월 27일, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorks_FullAccess

AWSOpsWorks_FullAccess는 AWS 관리형 정책으로, AWS OpsWorks에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorks_FullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 1월 22일, 16:29 UTC
- 편집된 시간: 2021년 1월 22일, 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs는 AWS 관리형 정책으로, 로그를 전송하고 필요한 로그 그룹을 생성하기 위해 CWLogs 통합을 활성화한 OpsWorks 인스턴스를 활성화합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksCloudWatchLogs를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 3월 30일, 17:47 UTC
- 편집된 시간: 2017년 3월 30일, 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksCMInstanceProfileRole

`AWSOpsWorksCMInstanceProfileRole`는 AWS 관리형 정책으로, OpsWorks CM에서 시작하는 인스턴스에 대한 S3 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSOpsWorksCMInstanceProfileRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 24일, 09:48 UTC
- 편집된 시간: 2021년 4월 23일, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksCMServiceRole

`AWSOpsWorksCMServiceRole`는 AWS 관리형 정책으로, OpsWorks CM 서버 생성에 사용되는 서비스 역할 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSOpsWorksCMServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 11월 24일, 09:49 UTC
- 편집된 시간: 2021년 4월 23일, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksInstanceRegistration

`AWSOpsWorksInstanceRegistration`는 AWS 관리형 정책으로, AWS OpsWorks 스택에 등록할 수 있도록 Amazon EC2 인스턴스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSOpsWorksInstanceRegistration`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 6월 3일, 14:23 UTC
- 편집된 시간: 2016년 6월 3일, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:RegisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksRegisterCLI_EC2

AWSOpsWorksRegisterCLI_EC2는 AWS 관리형 정책으로, OpsWorks CLI를 통해 EC2 인스턴스 등록을 활성화하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksRegisterCLI_EC2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 18일, 15:56 UTC
- 편집된 시간: 2019년 6월 18일, 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOpsWorksRegisterCLI_OnPremises

AWSOpsWorksRegisterCLI_OnPremises는 AWS 관리형 정책으로, OpsWorks CLI를 통해 온프레미스 인스턴스 등록을 활성화하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOpsWorksRegisterCLI_OnPremises를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 18일, 15:33 UTC
- 편집된 시간: 2019년 6월 18일, 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOrganizationsFullAccess

`AWSOrganizationsFullAccess`AWS Organizations에 대한 전체 액세스 권한을 AWS 제공하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSOrganizationsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 6일, 20:31 UTC
- 편집 시간: 2024년 2월 6일 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSOrganizationsReadOnlyAccess

`AWSOrganizationsReadOnlyAccess`AWS Organizations에 대한 읽기 전용 액세스를 AWS 제공하는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSOrganizationsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 6일, 20:32 UTC
- 편집 시간: 2024년 2월 6일 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSOrganizationsServiceTrustPolicy

`AWSOrganizationsServiceTrustPolicy`는 AWS 관리형 정책으로, AWS 서비스 Organizations가 고객 구성을 단순화할 목적으로 승인된 다른 AWS와 신뢰를 공유할 수 있도록 허용하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 10일, 23:04 UTC
- 편집된 시간: 2017년 11월 1일, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy는 AWS 관리형 정책으로, 이 정책은 온프레미스 네트워크에 Outpost 서버를 설치할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSOutpostsAuthorizeServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 1월 4일, 19:23 UTC
- 편집된 시간: 2023년 1월 4일, 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSOutpostsServiceRolePolicy

`AWSOutpostsServiceRolePolicy`는 AWS 관리형 정책으로, AWS Outposts에서 관리하는 AWS 리소스에 대한 액세스를 활성화하는 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 9일, 22:55 UTC
- 편집된 시간: 2020년 11월 9일, 22:55 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaApplianceRolePolicy

`AWSPanoramaApplianceRolePolicy`는 AWS 관리형 정책으로, AWS Panorama Appliance의 AWS IoT 소프트웨어가 Amazon CloudWatch에 로그를 업로드할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaApplianceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:13 UTC
- 편집된 시간: 2020년 12월 1일, 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaApplianceServiceRolePolicy

AWSPanoramaApplianceServiceRolePolicy는 AWS 관리형 정책으로, AWS Panorama Appliance가 Amazon CloudWatch에 로그를 업로드하고 AWS Panorama와 함께 사용하기 위해 생성된 Amazon S3 액세스 포인트에서 객체를 가져올 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaApplianceServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 10월 20일, 12:14 UTC
- 편집된 시간: 2023년 1월 17일, 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaFullAccess

`AWSPanoramaFullAccess`는 AWS 관리형 정책으로, AWS Panorama에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPanoramaFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 1일, 13:12 UTC
- 편집된 시간: 2022년 1월 12일, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
```

```
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaGreengrassGroupRolePolicy

`AWSPanoramaGreengrassGroupRolePolicy`는 AWS 관리형 정책으로, AWS Panorama Appliance의 AWS Lambda 함수가 Panorama에 있는 리소스를 관리하고, Amazon CloudWatch에 로그와 지표를 업로드하고, Panorama와 함께 사용하기 위해 생성된 버킷의 객체를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaGreengrassGroupRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:10 UTC
- 편집된 시간: 2021년 1월 6일, 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicy는 AWS 관리형 정책으로, Amazon SageMaker가 AWS Panorama와 함께 사용하기 위해 생성된 버킷의 객체를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaSageMakerRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:13 UTC
- 편집된 시간: 2020년 12월 1일, 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaServiceLinkedRolePolicy

`AWSPanoramaServiceLinkedRolePolicy`는 AWS 관리형 정책으로, AWS Panorama가 AWS IoT, AWS Secrets Manager 및 AWS Panorama의 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 10월 20일, 12:12 UTC
- 편집된 시간: 2021년 10월 20일, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy는 AWS 관리형 정책으로, AWS Panorama가 Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda, Amazon SageMaker 및 Amazon CloudWatch Logs의 리소스를 관리하고 AWS IoT, AWS IoT GreenGrass 및 Amazon SageMaker에 서비스 역할을 넘길 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPanoramaServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 12월 1일, 13:14 UTC
- 편집된 시간: 2020년 12월 1일, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPriceListServiceFullAccess

`AWSPriceListServiceFullAccess`는 AWS 관리형 정책으로, AWS Price List Service에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPriceListServiceFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 22일, 00:36 UTC
- 편집된 시간: 2017년 11월 22일, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateCAAuditor

`AWSPrivateCAAuditor`는 AWS 관리형 정책으로, AWS Private Certificate Authority에 대한 감사자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivateCAAuditor`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:33 UTC
- 편집된 시간: 2023년 2월 14일, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateCAFullAccess

`AWSPrivateCAFullAccess`는 AWS 관리형 정책으로, AWS Private Certificate Authority에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivateCAFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:20 UTC
- 편집된 시간: 2023년 2월 14일, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateCAPrivilegedUser

`AWSPrivateCAPrivilegedUser`는 AWS 관리형 정책으로, AWS Private Certificate Authority에 대한 권한 있는 인증서 사용자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivateCAPrivilegedUser`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:26 UTC
- 편집된 시간: 2023년 2월 14일, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateCAReadOnly

`AWSPrivateCAReadOnly`는 AWS 관리형 정책으로, AWS Private Certificate Authority에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivateCAReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:30 UTC
- 편집된 시간: 2023년 2월 14일, 18:30 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateCAUser

AWSPrivateCAUser는 AWS 관리형 정책으로, AWS Private Certificate Authority에 대한 인증서 사용자 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPrivateCAUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 2월 14일, 18:16 UTC
- 편집된 시간: 2023년 2월 14일, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAUser

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccess AWS Private Marketplace의 모든 관리 작업에 대한 전체 액세스 권한을 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPrivateMarketplaceAdminFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 16:32 UTC
- 편집 시간: 2024년 2월 14일 22:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSPrivateMarketplaceRequests

`AWSPrivateMarketplaceRequests`는 AWS 관리형 정책으로, AWS Private Marketplace에서 요청 생성에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSPrivateMarketplaceRequests`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 28일, 21:44 UTC
- 편집된 시간: 2019년 10월 28일, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPrivateNetworksServiceRolePolicy

`AWSPrivateNetworksServiceRolePolicy`는 AWS 관리형 정책으로, AWS Private Networks Service가 고객을 대신하여 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 12월 16일, 23:17 UTC
- 편집된 시간: 2021년 12월 16일, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonCodeBuildProvisioningBasicAccess

`AWSProtonCodeBuildProvisioningBasicAccess`는 AWS 관리형 정책으로, CodeBuild가 AWS Proton CodeBuild Provisioning을 위한 빌드를 실행하는 데 필요한 권한입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonCodeBuildProvisioningBasicAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 9일, 21:04 UTC
- 편집된 시간: 2022년 11월 9일, 21:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonCodeBuildProvisioningServiceRolePolicy

`AWSProtonCodeBuildProvisioningServiceRolePolicy`는 AWS 관리형 정책으로, AWS Proton이 사용자를 대신하여 CodeBuild 및 기타 AWS 서비스를 사용하여 Proton 리소스 프로비저닝을 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 9일, 21:32 UTC
- 편집된 시간: 2023년 5월 17일, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonDeveloperAccess

AWSProtonDeveloperAccess는 AWS 관리형 정책으로, AWS Proton API 및 관리 콘솔에 대한 액세스를 제공하지만 Proton 템플릿 또는 환경의 관리는 허용하지 않는 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSProtonDeveloperAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:02 UTC
- 편집된 시간: 2022년 11월 18일, 18:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
```

```
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonFullAccess

`AWSProtonFullAccess`는 AWS 관리형 정책으로, AWS Proton API 및 관리 콘솔에 대한 전체 액세스를 제공합니다. 이러한 권한 외에도 S3 버킷에서 템플릿 번들을 등록하려면 Amazon S3에 대한 액세스가 필요하며, Proton의 서비스 역할을 생성하고 관리하려면 Amazon IAM에 대한 액세스도 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSProtonFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:07 UTC
- 편집된 시간: 2022년 6월 20일, 12:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonReadOnlyAccess

`AWSProtonReadOnlyAccess`는 AWS 관리형 정책으로, AWS Proton API 및 관리 콘솔에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSProtonReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 2월 17일, 19:09 UTC
- 편집된 시간: 2022년 11월 18일, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonServiceGitSyncServiceRolePolicy

`AWSProtonServiceGitSyncServiceRolePolicy`는 AWS 관리형 정책으로, AWS Proton이 git 저장소의 서비스, 환경 및 구성 요소 정의를 AWS Proton으로 동기화할 수 있도록 허용하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 4일, 15:55 UTC
- 편집된 시간: 2023년 4월 4일, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy는 AWS 관리형 정책으로, AWS Proton이 git 리포지토리 콘텐츠를 Proton에 동기화하거나 Proton 콘텐츠를 git 리포지토리에 동기화할 수 있도록 허용하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 23일, 21:14 UTC
- 편집된 시간: 2021년 11월 23일, 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy AWS 관리형 정책으로, 결제 콘솔에서 구매 주문을 보고 수정할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSPurchaseOrdersServiceRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 6일, 18:15 UTC
- 편집된 시간: 2023년 7월 17일, 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuicksightAthenaAccess

`AWSQuicksightAthenaAccess`는 AWS 관리형 정책으로, Athena 쿼리 결과에 사용되는 Athena API 및 S3 버킷에 대한 Quicksight 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSQuicksightAthenaAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 12월 9일, 02:31 UTC
- 편집된 시간: 2021년 7월 7일, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
```

```
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightDescribeRDS

`AWSQuickSightDescribeRDS`는 AWS 관리형 정책으로, QuickSight가 RDS 리소스를 설명할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightDescribeRDS를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:24 UTC
- 편집된 시간: 2015년 11월 10일, 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightDescribeRedshift

AWSQuickSightDescribeRedshift는 AWS 관리형 정책으로, QuickSight가 Redshift 리소스를 설명할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightDescribeRedshift를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:25 UTC
- 편집된 시간: 2015년 11월 10일, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy는 AWS 관리형 정책으로, Amazon QuickSight에서 Amazon Elasticsearch 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightElasticsearchPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 9월 9일, 17:27 UTC
- 편집된 시간: 2021년 9월 7일, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightIoTAnalyticsAccess

`AWSQuickSightIoTAnalyticsAccess`는 AWS 관리형 정책으로, QuickSight에 IoT Analytics 데이터세트에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSQuickSightIoTAnalyticsAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 17:00 UTC
- 편집된 시간: 2017년 11월 29일, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightListIAM

AWSQuickSightListIAM는 AWS 관리형 정책으로, QuickSight가 IAM 엔티티를 나열할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSQuickSightListIAM를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 11월 10일, 23:25 UTC
- 편집된 시간: 2015년 11월 10일, 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuicksightOpenSearchPolicy

`AWSQuicksightOpenSearchPolicy`는 AWS 관리형 정책으로, Amazon QuickSight에서 Amazon OpenSearch 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSQuicksightOpenSearchPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2021년 9월 7일, 23:26 UTC
- 편집된 시간: 2021년 9월 7일, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightSageMakerPolicy

`AWSQuickSightSageMakerPolicy`는 AWS 관리형 정책으로, Amazon QuickSight에서 Amazon SageMaker 리소스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSQuickSightSageMakerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 1월 17일, 17:18 UTC

- 편집된 시간: 2023년 10월 30일, 17:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSQuickSightTimestreamPolicy

`AWSQuickSightTimestreamPolicy`는 AWS 관리형 정책으로, AWS Timestream API에 대한 AWS QuickSight 액세스입니다. 고객은 이 정책을 AWS QuickSight 역할에 연결하여 데이터 및 메타데이터 검색을 허용할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSQuickSightTimestreamPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 9월 30일, 21:47 UTC
- 편집된 시간: 2020년 9월 30일, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSReachabilityAnalyzerServiceRolePolicy

`AWSReachabilityAnalyzerServiceRolePolicy`는 AWS 관리형 정책으로, VPC Reachability Analyzer가 사용자를 대신하여 AWS 리소스에 액세스하고 AWS Organizations와 통합할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 23일, 17:12 UTC
- 편집된 시간: 2023년 6월 23일, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRefactoringToolkitFullAccess

`AWSRefactoringToolkitFullAccess`는 AWS 관리형 정책으로, 이 정책은 Microsoft Visual Studio용 AWS Toolkit 리팩터링 확장 프로그램과 함께 AWS 서비스를 사용할 수 있는 권한을 부여합니다. 로컬 AWS 프로필에 연결되도록 고안되었습니다. 이 정책은 Amazon S3에 애플리케이션 아티팩트를 업로드하고 Amazon S3에서 결과 아티팩트를 다운로드할 수 있도록 허용합니다. Amazon Elastic Container Registry (Amazon ECR) 를 사용하여 이미지를 저장 AWS CodeBuild 및 검색하고 이를 통해 컨테이너 이미지로 애플리케이션을 구축할 수 있습니다. 또한 Amazon Elastic Container Service(Amazon ECS)와 같은 AWS의 컨테이너 서비스에 애플리케이션을 배포하고, VPC 리소스를 선택적으로 생성하고, AWS Directory Service와 같은 기존 인프라에 선택적으로 연결하고, 기타 관련 서비스를 사용할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSRefactoringToolkitFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 10월 25일, 16:41 UTC
- 편집 시간: 2023년 11월 18일 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
```

```
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CodeBuildExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Sid" : "CreateSecurityGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2CreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2CreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccessATS",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "EcsModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsReadTaskDefinitionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecar",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecarATS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Sid" : "CreateEcsServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CloudwatchCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "SsmParameterAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
```

```
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
```

```
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetECSSLR",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Sid" : "PortingAssistantFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Sid" : "ApplicationTransformationAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Sid" : "EcrPushAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrAuthAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRefactoringToolkitSidecarPolicy

`AWSRefactoringToolkitSidecarPolicy`는 AWS 관리형 정책으로, 이 정책은 Microsoft Visual Studio의 .NET Refactoring 확장 프로그램용 AWS Toolkit을 사용하여 AWS에서 애플리케이션을 테스트하기 위해 생성된 Amazon ECS Tasks에서 사용하도록 고안되었습니다. 이 정책은 Amazon S3에서 애플리케이션 아티팩트를 다운로드하고, AWS Systems Manager를 사용하여 태스크 상태를 전달하고, 기타 필요한 서비스에 액세스할 수 있는 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSRefactoringToolkitSidecarPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 10월 25일, 16:41 UTC
- 편집된 시간: 2022년 10월 29일, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSrePostPrivateCloudWatchAccess

`AWSrePostPrivateCloudWatchAccess`메트릭 데이터를 게시하기 위한 re:Post Private 액세스를 제공하는 AWS관리형 정책입니다. CloudWatch

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 15일, 16:37 UTC
- 편집된 시간: 2023년 11월 15일, 16:37 UTC

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

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicy는 다음과 같은 AWS관리형 정책입니다. 이 정책을 통해 re:Post Space 서비스는 Space 응용 프로그램을 통해 생성된 Support 사례를 생성, 관리 및 해결할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSRepostSpaceSupportOperationsPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 11월 26일, 21:52 UTC
- 편집 시간: 2023년 11월 26일, 21:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
```

```
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResilienceHubAsssessmentExecutionPolicy

`AWSResilienceHubAsssessmentExecutionPolicy`는 AWS 관리형 정책으로, 평가를 실행하기 위해 다른 AWS 서비스에 대한 액세스를 허용하는 AWS Resilience Hub 서비스 역할에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSResilienceHubAsssessmentExecutionPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 6월 27일, 12:32 UTC
- 편집된 시간: 2023년 10월 29일, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
```

```
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "s3:GetBucketLocation",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3Statement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceAccessManagerFullAccess

`AWSResourceAccessManagerFullAccess`는 AWS 관리형 정책으로, AWS Resource Access Manager에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSResourceAccessManagerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 4일, 17:28 UTC
- 편집된 시간: 2019년 6월 4일, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceAccessManagerReadOnlyAccess

`AWSResourceAccessManagerReadOnlyAccess`는 AWS 관리형 정책으로, AWS Resource Access Manager에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSResourceAccessManagerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 9일, 20:58 UTC
- 편집된 시간: 2019년 12월 9일, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceAccessManagerResourceShareParticipantAccess

`AWSResourceAccessManagerResourceShareParticipantAccess`는 AWS 관리형 정책으로, 리소스 공유 참여자에게 필요한 AWS Resource Access Manager API에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSResourceAccessManagerResourceShareParticipantAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 9일, 20:41 UTC
- 편집된 시간: 2019년 12월 9일, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceAccessManagerServiceRolePolicy

`AWSResourceAccessManagerServiceRolePolicy`는 AWS 관리형 정책으로, 고객의 Organizations 구조에 대한 읽기 전용 AWS Resource Access Manager 액세스를 포함하는 정책입니다. 또한 역할을 자체 삭제할 수 있는 IAM 권한도 포함합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 19:28 UTC
- 편집된 시간: 2018년 11월 14일, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess는 AWS 관리형 정책으로, 이 정책은 Resource Explorer에 리소스에 액세스할 수 있는 관리자 권한을 부여하고 이 액세스를 지원하기 위해 다른 AWS 서비스에 읽기 전용 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceExplorerFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 7일, 20:01 UTC
- 편집된 시간: 2023년 11월 14일, 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceExplorerOrganizationsAccess

`AWSResourceExplorerOrganizationsAccess`는 AWS 관리형 정책으로, 이 정책은 Resource Explorer에 관리자 권한을 부여하고 이 액세스를 지원하기 위해 다른 AWS 서비스에 읽기 전용 권한을 부여합니다. AWS Organizations 관리자가 콘솔에서 다중 계정 검색을 설정하고 관리하려면 이러한 권한이 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSResourceExplorerOrganizationsAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 14일, 17:01 UTC
- 편집된 시간: 2023년 11월 14일, 17:01 UTC

- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceExplorerReadOnlyAccess

AWSResourceExplorerReadOnlyAccess는 AWS 관리형 정책으로, 이 정책은 Resource Explorer 리소스를 검색하고 볼 수 있는 읽기 전용 권한을 부여하고 이 액세스를 지원하기 위해 다른 AWS 서비스에 읽기 전용 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceExplorerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 7일, 19:56 UTC
- 편집된 시간: 2023년 11월 14일, 16:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicy리소스 탐색기가 사용자를 대신하여 리소스 및 CloudTrail 이벤트를 보고 검색할 리소스를 인덱싱하도록 허용하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 10월 25일, 20:35 UTC
- 편집 시간: 2023년 12월 20일 13:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/deployments"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
```

```
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeguru-profiler:ListProfilingGroups",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
```

```
        "databrew:ListDatasets",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "detective:ListGraphs",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
```

```
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr:DescribeRepositories",
        "ecr-public:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
```

```
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetLabels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "gamelift:ListAliases",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "greengrass:ListComponents",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
```

```
        "greengrass:ListComponentVersions",
        "greengrass:ListGroups",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iot:ListJobTemplates",
        "iot:ListAuthorizers",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListSecurityProfiles",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
```

```
        "iottwinmaker:ListWorkspaces",
        "kafka:ListConfigurations",
        "kms:ListKeys",
        "ivs:ListChannels",
        "ivs:ListStreamKeys",
        "kafka:ListClusters",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListStreams",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lookoutmetrics:ListAlerts",
        "lookoutvision:ListProjects",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mq:ListBrokers",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
```

```
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverRules",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListStorageLensConfigurations",
        "sagemaker:ListModels",
        "sagemaker:ListNotebookInstances",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm-incidents:ListResponsePlans",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "timestream:ListDatabases",
        "wisdom:listAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:listKnowledgeBases"
      ],
      "Resource" : [
```

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

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSResourceGroupsReadOnlyAccess

AWSResourceGroupsReadOnlyAccess는 AWS 관리형 정책으로, AWS Resource Groups에 대한 읽기 전용 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSResourceGroupsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 10:27 UTC
- 편집된 시간: 2019년 2월 5일, 17:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRoboMaker_FullAccess

`AWSRoboMaker_FullAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 AWS RoboMaker에 대한 전체 액세스를 제공합니다. 또한 관련 서비스(예: S3, IAM)에 대한 선택적 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSRoboMaker_FullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 10일, 18:34 UTC
- 편집된 시간: 2021년 9월 16일, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRoboMakerReadOnlyAccess

`AWSRoboMakerReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console 및 SDK를 통해 AWS RoboMaker에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSRoboMakerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 26일, 05:30 UTC
- 편집된 시간: 2020년 8월 28일, 23:10 UTC

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

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRoboMakerServicePolicy

`AWSRoboMakerServicePolicy`는 AWS 관리형 정책으로, RoboMaker 서비스 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 06:30 UTC
- 편집된 시간: 2021년 11월 11일, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

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

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRoboMakerServiceRolePolicy

`AWSRoboMakerServiceRolePolicy`는 AWS 관리형 정책으로, RoboMaker 서비스 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSRoboMakerServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 26일, 05:33 UTC
- 편집된 시간: 2018년 11월 26일, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSRolesAnywhereServicePolicy

AWSRolesAnywhereServicePolicy는 IAWS 관리형 정책으로, AM Roles Anywhere가 CloudWatch에 서비스/사용 지표를 게시하고 사용자를 대신하여 Private Certificate Authorities의 상태를 확인할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 7월 5일, 15:26 UTC
- 편집된 시간: 2022년 7월 5일, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "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:*:*:*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy는 AWS 관리형 정책으로, Amazon S3 on Outposts 서비스가 사용자를 대신하여 EC2 네트워크 리소스를 관리하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 10월 3일, 20:32 UTC
- 편집된 시간: 2023년 10월 3일, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSavingsPlansFullAccess

AWSSavingsPlansFullAccess는 AWS 관리형 정책으로, 절감형 플랜 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSavingsPlansFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 6일, 22:45 UTC
- 편집된 시간: 2019년 11월 6일, 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess는 AWS 관리형 정책으로, 절감형 플랜 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSavingsPlansReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 6일, 22:45 UTC
- 편집된 시간: 2019년 11월 6일, 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess`는 AWS 관리형 정책으로, AWS Security Hub를 사용할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSecurityHubFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2018년 11월 27일, 23:54 UTC
- 편집 시간: 2023년 11월 16일 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess`는 AWS 관리형 정책으로, 조직 내에서 AWS Security Hub를 활성화하고 관리할 수 있는 권한을 부여합니다. 조직 전체에서 서비스를 활성화하고 서비스에 대한 위임된 관리자 계정을 결정하는 작업이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSecurityHubOrganizationsAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2021년 3월 15일, 20:53 UTC
- 편집 시간: 2023년 11월 16일 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` AWS Security Hub 리소스에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSecurityHubReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 28일, 01:34 UTC
- 편집 시간: 2024년 2월 22일 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy는 AWS 관리형 정책으로, AWS Security Hub가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2018년 11월 27일, 23:47 UTC
- 편집 시간: 2023년 11월 27일 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

정책 버전

정책 버전: v14(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogAdminFullAccess

`AWSServiceCatalogAdminFullAccess`은 AWS 관리형 정책으로, Service Catalog 관리 기능에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSServiceCatalogAdminFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 15일, 17:19 UTC
- 편집된 시간: 2023년 4월 13일, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogAdminReadOnlyAccess

AWSServiceCatalogAdminReadOnlyAccess은 AWS 관리형 정책으로, Service Catalog 관리 기능에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAdminReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 25일, 18:53 UTC
- 편집된 시간: 2019년 10월 25일, 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccess은 AWS 관리형 정책으로, Service Catalog App Registry 기능에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAppRegistryFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 12일, 22:25 UTC
- 편집 시간: 2023년 12월 7일, 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*:*:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogAppRegistryReadOnlyAccess

AWSServiceCatalogAppRegistryReadOnlyAccess은 AWS 관리형 정책으로, Service Catalog App Registry 기능에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogAppRegistryReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 12일, 22:34 UTC
- 편집된 시간: 2022년 11월 17일, 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogAppRegistryServiceRolePolicy

`AWSServiceCatalogAppRegistryServiceRolePolicy`는 AWS 관리형 정책으로, Service Catalog AppRegistry가 사용자를 대신하여 리소스 그룹을 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 5월 18일, 22:18 UTC
- 편집된 시간: 2022년 10월 26일, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess은 AWS 관리형 정책으로, Service Catalog 최종 사용자 기능에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSServiceCatalogEndUserFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 2월 15일, 17:22 UTC
- 편집된 시간: 2019년 7월 10일, 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogEndUserReadOnlyAccess

`AWSServiceCatalogEndUserReadOnlyAccess`은 AWS 관리형 정책으로, Service Catalog 최종 사용자 기능에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSServiceCatalogEndUserReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 10월 25일, 18:49 UTC
- 편집된 시간: 2019년 10월 25일, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`는 AWS 관리형 정책으로, AWS Organizations의 조직 구조와 동기화하기 위한 AWS ServiceCatalog에 대한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 10일, 20:48 UTC
- 편집된 시간: 2023년 4월 10일, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceCatalogSyncServiceRolePolicy

`AWSServiceCatalogSyncServiceRolePolicy`는 AWS 관리형 정책으로, 소스 리포지토리에서 프로비저닝 아티팩트를 동기화하기 위한 AWS ServiceCatalog의 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 15일, 21:20 UTC
- 편집된 시간: 2022년 11월 15일, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForAmazonEKSNodegroup

AWSServiceRoleForAmazonEKSNodegroup는 AWS 관리형 정책으로, 고객 계정의 노드 그룹을 관리하는 데 필요한 권한입니다. 이러한 정책은 다음 리소스의 관리와 관련이 있습니다: AutoscalingGroups SecurityGroups, LaunchTemplates 및 InstanceProfiles.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 7일, 01:34 UTC
- 편집 시간: 2024년 1월 4일 20:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToManageEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`는 AWS 관리형 정책으로, CloudWatch 경보에서 사용하는 Systems Manager 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 10월 1일, 09:49 UTC
- 편집된 시간: 2020년 10월 1일, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy는 AWS 관리형 정책으로, CloudWatch가 사용자를 대신하여 RDS Performance Insights 지표에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 9월 7일, 09:32 UTC
- 편집된 시간: 2023년 9월 7일, 09:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForCodeGuru-Profiler

`AWSServiceRoleForCodeGuru-Profiler`는 AWS 관리형 정책으로, Amazon CodeGuru Profiler가 사용자를 대신하여 알림을 보내기 위해 필요한 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 26일, 22:04 UTC
- 편집된 시간: 2020년 6월 26일, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForCodeWhispererPolicy

`AWSServiceRoleForCodeWhispererPolicy`는 다음과 같은 AWS 관리형 정책입니다. 이 역할은 청구 계산을 CodeWhisperer 위해 계정의 데이터에 액세스할 수 있는 권한을 부여하고, Amazon에서 보안 보고서를 생성 및 액세스할 수 있는 권한을 제공하고 CodeGuru, Amazon에서 데이터를 내보낼 수 있는 권한을 부여합니다. CloudWatch

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 24일, 19:39 UTC
- 편집 시간: 2024년 3월 1일 23:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책을 사용하는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
```

```
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
```

```
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSServiceRoleForEC2ScheduledInstances

`AWSServiceRoleForEC2ScheduledInstances`는 AWS 관리형 정책으로, EC2 Scheduled Instances가 스팟 인스턴스를 시작하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 10월 12일, 18:31 UTC
- 편집된 시간: 2017년 10월 12일, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy는 AWS 관리형 정책으로, AWS GroundStation은 이 서비스 연결 역할을 사용하여 EC2를 호출하여 퍼블릭 IPv4 주소를 찾습니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 12월 13일, 23:52 UTC
- 편집된 시간: 2022년 12월 13일, 23:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForImageBuilder

`AWSServiceRoleForImageBuilder`는 AWS 관리형 정책으로, EC2ImageBuilder가 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 29일, 22:02 UTC
- 편집된 시간: 2023년 10월 19일, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

정책 버전

정책 버전: v19(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
```

```
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
```

```
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
```

```
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
```

```
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForIoTSiteWise

AWSServiceRoleForIoTSiteWise는 AWS IoT가 게이트웨이와 쿼리 데이터를 프로비저닝하고 관리할 수 있도록 SiteWise 하는 AWS관리형 정책입니다. 이 정책에는 그룹에 배포하는 데 필요한 필수 AWS Greengrass 권한, 서비스 접두사가 붙은 함수를 생성 및 업데이트하는 데 필요한 AWS Lambda 권한, 데이터스토어에서 데이터를 쿼리하는 데 필요한 IoT AWS Analytics 권한이 포함됩니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 14일, 19:19 UTC
- 편집된 시간: 2023년 11월 13일, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy는 AWS 관리형 정책으로, 로그 전송 서비스가 사용자를 대신하여 로그 대상을 호출하여 로그를 전달할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 4일, 17:31 UTC
- 편집된 시간: 2021년 7월 15일, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForMonitronPolicy

`AWSServiceRoleForMonitronPolicy`는 AWS 관리형 정책으로, Amazon Monitron에 사용자를 대신하여 AWS SSO 사용자 할당을 포함한 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 2일, 19:06 UTC
- 편집된 시간: 2022년 9월 29일, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForNeptuneGraphPolicy

`AWSServiceRoleForNeptuneGraphPolicy`다음과 같은 AWS관리형 정책으로, Amazon Neptune에 대한 운영 및 사용 지표와 로그를 게시할 수 있는 Cloudwatch 액세스 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 29일, 14:03 UTC
- 편집 시간: 2023년 11월 29일, 14:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRoleForPrivateMarketplaceAdminPolicy

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`Private Marketplace 리소스를 설명 및 업데이트하고 AWS Organizations를 설명할 수 있는 권한을 제공하는 AWS 관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 작성 시간: 2024년 2월 14일 22:28 UTC
- 편집 시간: 2024년 2월 14일 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSServiceRoleForSMS

AWSServiceRoleForSMS는 AWS 관리형 정책으로, EC2, S3 및 Cloudformation을 AWS 포함하여 서비스 인스턴스를 마이그레이션하는 데 필요한 AWS 서비스 및 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 6일, 18:39 UTC
- 편집된 시간: 2020년 10월 15일, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

정책 버전

정책 버전: v10(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRolePolicyForBackupReports

`AWSServiceRolePolicyForBackupReports`는 AWS 관리형 정책으로, 사용자를 대신하여 규정 준수 보고서를 생성할 수 있는 AWS Backup 권한을 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 19일, 21:16 UTC

- 편집된 시간: 2023년 3월 10일, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting는 AWS 관리형 정책으로, 이 정책에는 복원을 테스트하고 테스트 중에 생성된 리소스를 정리할 수 있는 권한이 포함되어 있습니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2023년 11월 10일, 23:37 UTC
- 편집 시간: 2024년 2월 14일 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy는 AWS 관리형 정책으로, 심각도가 높은 이벤트 발생 시 AWS DDoS 대응팀에 DDoS 공격 완화를 지원할 수 있는 사용자 AWS 계정에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSShieldDRTAccessPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 6월 5일, 22:29 UTC
- 편집된 시간: 2020년 12월 15일, 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSShieldServiceRolePolicy

AWSShieldServiceRolePolicy는 AWS 관리형 정책으로, AWS Shield가 사용자를 대신하여 AWS 리소스에 액세스하여 DDoS 보호를 제공하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 11월 17일, 19:17 UTC
- 편집된 시간: 2021년 11월 17일, 19:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
```

```
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSMForSAPServiceLinkedRolePolicy

`AWSSSMForSAPServiceLinkedRolePolicy`는 AWS 관리형 정책으로, SAP 소프트웨어를 관리하고 AWS와 통합하는 데 필요한 권한을 AWS Systems Manager에 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 16일, 01:18 UTC
- 편집 시간: 2023년 11월 21일 03:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
```

```
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
```

```
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
```

```
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy는 AWS 관리형 정책으로, 서비스 연결 역할 정책, 서비스 연결 역할 AWSServiceRoleForAmazonSSM_OpsInsights에 대한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 6월 16일, 20:12 UTC
- 편집된 시간: 2021년 6월 16일, 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator는 AWS 관리형 정책으로, SSO 디렉터리에 대한 관리자 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSODirectoryAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 31일, 23:54 UTC
- 편집된 시간: 2022년 10월 20일, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```


자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly는 AWS 관리형 정책으로, SSO 디렉터리에 대한 읽기 전용 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSODirectoryReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 10월 31일, 23:49 UTC
- 편집된 시간: 2022년 11월 16일, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator`는 AWS 관리형 정책으로, AWS SSO 내에서 AWS Organizations의 마스터 및 멤버 계정과 클라우드 애플리케이션을 관리하기 위한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSSOMasterAccountAdministrator`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:36 UTC
- 편집된 시간: 2022년 10월 20일, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
```

```
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator는 AWS 관리형 정책으로, AWS SSO 내에서 AWS Organizations의 멤버 계정과 클라우드 애플리케이션을 관리하기 위한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSOMemberAccountAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:45 UTC
- 편집된 시간: 2022년 10월 20일, 20:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
```

```
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSOReadOnly

AWSSSOReadOnly는 AWS 관리형 정책으로, AWS SSO 구성에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSSOReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 27일, 20:24 UTC
- 편집된 시간: 2022년 8월 22일, 17:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSSOServiceRolePolicy

`AWSSSOServiceRolePolicy`는 AWS 관리형 정책으로, AWS SSO에 사용자를 대신하여 IAM 역할, 정책, SAML IdP를 포함한 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2017년 12월 5일, 18:36 UTC
- 편집된 시간: 2022년 10월 20일, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess는 AWS 관리형 정책으로, AWS StepFunctions 콘솔에 대한 사용자/역할/기타 액세스를 제공하기 위한 액세스 정책입니다. 전체 콘솔 환경을 위해서는 이 정책 외에도 사용자에게 서비스에서 위임할 수 있는 다른 IAM 역할에 대한 IAM:PassRole 권한이 필요할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSStepFunctionsConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:54 UTC
- 편집된 시간: 2017년 1월 12일, 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStepFunctionsFullAccess

`AWSStepFunctionsFullAccess`는 AWS 관리형 정책으로, AWS StepFunctions API에 대한 사용자/역할/기타 액세스를 제공하기 위한 액세스 정책입니다. 전체 액세스를 위해서는 이 정책 외에도 사용자에게 서비스에서 위임할 수 있는 하나 이상의 IAM 역할에 대한 iam:PassRole 권한이 있어야 합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSStepFunctionsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:51 UTC
- 편집된 시간: 2017년 1월 11일, 21:51 UTC

- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStepFunctionsReadOnlyAccess

`AWSStepFunctionsReadOnlyAccess`는 AWS 관리형 정책으로, AWS StepFunctions 서비스에 대한 사용자/역할/기타 읽기 전용 액세스를 제공하기 위한 액세스 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSStepFunctionsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 1월 11일, 21:46 UTC
- 편집된 시간: 2017년 11월 10일, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStorageGatewayFullAccess

AWSStorageGatewayFullAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Storage Gateway에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSStorageGatewayFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2022년 9월 6일, 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStorageGatewayReadOnlyAccess

`AWSStorageGatewayReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Storage Gateway에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSStorageGatewayReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2022년 9월 6일, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSStorageGatewayServiceRolePolicy

`AWSStorageGatewayServiceRolePolicy`는 AWS 관리형 정책으로, Storage Gateway가 다른 서비스를 AWS Storage Gateway와 통합할 수 있도록 하는 데 사용하는 AWS 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 2월 17일, 19:03 UTC
- 편집된 시간: 2021년 2월 17일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess공급망 애플리케이션 내에서 작업을 수행하는 데 필요한 권한을 포함하여 AWS 공급망 연동 사용자에게 AWS 공급망 애플리케이션에 대한 액세스 권한을 AWSSupplyChainFederationAdminAccess 제공하는 AWS관리형 정책입니다. AWS 이 정책은 IAM Identity Center 사용자 및 그룹에 대한 관리 권한을 제공하며 AWS Supply Chain이 사용자를 대신하여 생성한 역할에 연결됩니다. AWSSupplyChainFederationAdminAccess 정책을 다른 IAM 엔티티에 연결해서는 안 됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupplyChainFederationAdminAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 3월 1일, 18:54 UTC
- 편집된 시간: 2023년 11월 1일, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
```

```
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportAccess

`AWSSupportAccess`는 AWS 관리형 정책으로, 사용자가 AWS Support Center에 액세스할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSupportAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC

- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportAppFullAccess

`AWSSupportAppFullAccess`는 AWS 관리형 정책으로, AWS Support 앱과 AWS Support 및 Service Quotas와 같은 기타 필수 서비스에 대한 전체 액세스를 제공합니다. 이 정책에는 사용자가 지

원 사례를 위해 AWS Support에 문의하고, 서비스 할당량을 변경하고, 관련 서비스 연결 역할을 생성할 수 있도록 지원 서비스를 사용할 수 있는 권한이 포함되어 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportAppFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 22일, 16:53 UTC
- 편집된 시간: 2022년 8월 22일, 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportAppReadOnlyAccess

`AWSSupportAppReadOnlyAccess`는 AWS 관리형 정책으로, AWS Support App에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSupportAppReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 22일, 17:01 UTC
- 편집된 시간: 2022년 8월 22일, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportPlansFullAccess

AWSSupportPlansFullAccess는 AWS 관리형 정책으로, 지원 플랜에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportPlansFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 9월 27일, 18:19 UTC
- 편집된 시간: 2023년 5월 9일, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportPlansReadOnlyAccess

AWSSupportPlansReadOnlyAccess는 AWS 관리형 정책으로, 지원 플랜에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSSupportPlansReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 9월 27일, 18:08 UTC
- 편집된 시간: 2022년 9월 27일, 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSupportServiceRolePolicy

`AWSSupportServiceRolePolicy`는 AWS 관리형 정책으로, AWS Support가 청구, 관리 및 지원 서비스를 제공하기 위해 AWS 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 4월 19일, 18:04 UTC
- 편집 시간: 2024년 1월 17일 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

정책 버전

정책 버전: v34(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
```

```
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActions",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
```

```
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
```

```
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
```

```
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
```

```
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
```

```
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeWarmPool",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listTags",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
```

```
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:listJobs",
        "braket:getDevice",
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
```

```
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
```

```
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
```

```
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listStreamingDistributions",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
```

```
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
```

```
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listWebhooks",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
```

```
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getEnrollmentStatus",
```

```
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
```

```
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
```

```
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
```

```
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
```

```
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
```

```
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
```

```
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
```

```
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
```

```
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
```

```
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImages",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
```

```
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
```

```
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
```

```
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
```

```
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegments",
        "evidently:listSegmentReferences",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listArchives",
        "events:listApiDestinations",
        "events:listConnections",
        "events:listEndpoints",
```

```
            "events:listEventBuses",
            "events:listEventSources",
            "events:listPartnerEventSourceAccounts",
            "events:listPartnerEventSources",
            "events:listReplays",
            "events:listRuleNamesByTarget",
            "events:listRules",
            "events:listTargetsByRule",
            "events:testEventPattern",
            "firehose:describeDeliveryStream",
            "firehose:listDeliveryStreams",
            "fms:getAdminAccount",
            "fms:getComplianceDetail",
            "fms:getNotificationChannel",
            "fms:getPolicy",
            "fms:getProtectionStatus",
            "fms:listComplianceStatus",
            "fms:listMemberAccounts",
            "fms:listPolicies",
            "forecast:describeDataset",
            "forecast:describeDatasetGroup",
            "forecast:describeDatasetImportJob",
            "forecast:describeForecast",
            "forecast:describeForecastExportJob",
            "forecast:describePredictor",
            "forecast:getAccuracyMetrics",
            "forecast:listDatasetGroups",
            "forecast:listDatasetImportJobs",
            "forecast:listDatasets",
            "forecast:listForecastExportJobs",
            "forecast:listForecasts",
            "forecast:listPredictors",
            "fsx:describeBackups",
            "fsx:describeDataRepositoryAssociations",
            "fsx:describeDataRepositoryTasks",
            "fsx:describeFileCaches",
            "fsx:describeFileSystems",
            "fsx:describeSnapshots",
            "fsx:describeStorageVirtualMachines",
            "fsx:describeVolumes",
            "fsx:listTagsForResource",
            "gamelift:describeAlias",
            "gamelift:describeBuild",
            "gamelift:describeEC2InstanceLimits",
```

```
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
```

```
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
```

```
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
```

```
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:getDetector",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMasterAccount",
        "guardduty:getMembers",
        "guardduty:getThreatIntelSet",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
```

```
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
```

```
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflowStepExecutions",
        "imagebuilder:listTagsForResource",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
```

```
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "inspector-scan:scanSbom",
        "internetmonitor:getMonitor",
        "internetmonitor:listMonitors",
        "internetmonitor:getHealthEvent",
        "internetmonitor:listHealthEvents",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
```

```
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getFleet",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifests",
```

```
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listVehicles",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
```

```
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:getBootstrapBrokers",
        "kafka:listConfigurations",
        "kafka:listConfigurationRevisions",
        "kafka:listClusterOperations",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listNodes",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
```

```
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreams",
        "kinesis:listStreamConsumers",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
```

```
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
```

```
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
```

```
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
```

```
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:listLogDeliveries",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
```

```
        "macie2:listFindings",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:listChannels",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
```

```
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
```

```
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
```

```
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "nimble:getEula",
        "nimble:getLaunchProfile",
        "nimble:getLaunchProfileDetails",
        "nimble:getLaunchProfileInitialization",
        "nimble:getLaunchProfileMember",
        "nimble:getStreamingImage",
        "nimble:getStreamingSession",
        "nimble:getStreamingSessionStream",
        "nimble:getStudio",
        "nimble:getStudioComponent",
        "nimble:listEulaAcceptances",
        "nimble:listEulas",
        "nimble:listLaunchProfiles",
        "nimble:listStreamingImages",
        "nimble:listStreamingSessions",
        "nimble:listStudioComponents",
        "nimble:listStudios",
        "notifications:getEventRule",
```

```
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferenceStores",
        "omics:listReferences",
        "omics:listRunGroups",
        "omics:listRunTasks",
        "omics:listRuns",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
```

```
        "omics:listWorkflows",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:listAccounts",
        "organizations:listTagsForResource",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
```

```
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworks",
        "private-networks:listNetworkResources",
```

```
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
```

```
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
```

```
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
```

```
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
```

```
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
```

```
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
```

```
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
```

```
            "s3:getObjectRetention",
            "s3:getReplicationConfiguration",
            "s3:getStorageLensConfiguration",
            "s3:listAccessPoints",
            "s3:listAccessPointsForObjectLambda",
            "s3:listAllMyBuckets",
            "s3:listBucket",
            "s3:listBucketMultipartUploads",
            "s3:listBucketVersions",
            "s3:listJobs",
            "s3:listMultipartUploadParts",
            "s3:listMultiRegionAccessPoints",
            "s3:listStorageLensConfigurations",
            "s3express:listAllMyDirectoryBuckets",
            "sagemaker:describeAction",
            "sagemaker:describeAlgorithm",
            "sagemaker:describeApp",
            "sagemaker:describeAppImageConfig",
            "sagemaker:describeArtifact",
            "sagemaker:describeAutoMLJob",
            "sagemaker:describeCodeRepository",
            "sagemaker:describeCompilationJob",
            "sagemaker:describeContext",
            "sagemaker:describeDataQualityJobDefinition",
            "sagemaker:describeDevice",
            "sagemaker:describeDeviceFleet",
            "sagemaker:describeDomain",
            "sagemaker:describeEdgeDeploymentPlan",
            "sagemaker:describeEdgePackagingJob",
            "sagemaker:describeEndpoint",
            "sagemaker:describeEndpointConfig",
            "sagemaker:describeExperiment",
            "sagemaker:describeFeatureGroup",
            "sagemaker:describeFeatureMetadata",
            "sagemaker:describeFlowDefinition",
            "sagemaker:describeHub",
            "sagemaker:describeHubContent",
            "sagemaker:describeHumanTaskUi",
            "sagemaker:describeHyperParameterTuningJob",
            "sagemaker:describeImage",
            "sagemaker:describeImageVersion",
            "sagemaker:describeInferenceExperiment",
            "sagemaker:describeInferenceRecommendationsJob",
            "sagemaker:describeLabelingJob",
```

```
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
```

```
            "sagemaker:listDomains",
            "sagemaker:listEdgeDeploymentPlans",
            "sagemaker:listEdgePackagingJobs",
            "sagemaker:listEndpointConfigs",
            "sagemaker:listEndpoints",
            "sagemaker:listExperiments",
            "sagemaker:listFeatureGroups",
            "sagemaker:listFlowDefinitions",
            "sagemaker:listHubContents",
            "sagemaker:listHubContentVersions",
            "sagemaker:listHubs",
            "sagemaker:listHumanTaskUis",
            "sagemaker:listHyperParameterTuningJobs",
            "sagemaker:listImages",
            "sagemaker:listImageVersions",
            "sagemaker:listInferenceExperiments",
            "sagemaker:listInferenceRecommendationsJobs",
            "sagemaker:listInferenceRecommendationsJobSteps",
            "sagemaker:listLabelingJobs",
            "sagemaker:listLabelingJobsForWorkteam",
            "sagemaker:listLineageGroups",
            "sagemaker:listModelBiasJobDefinitions",
            "sagemaker:listModelCardExportJobs",
            "sagemaker:listModelCards",
            "sagemaker:listModelCardVersions",
            "sagemaker:listModelExplainabilityJobDefinitions",
            "sagemaker:listModelMetadata",
            "sagemaker:listModelPackageGroups",
            "sagemaker:listModelPackages",
            "sagemaker:listModelQualityJobDefinitions",
            "sagemaker:listModels",
            "sagemaker:listMonitoringAlertHistory",
            "sagemaker:listMonitoringAlerts",
            "sagemaker:listMonitoringExecutions",
            "sagemaker:listMonitoringSchedules",
            "sagemaker:listNotebookInstanceLifecycleConfigs",
            "sagemaker:listNotebookInstances",
            "sagemaker:listPipelineExecutions",
            "sagemaker:listPipelineExecutionSteps",
            "sagemaker:listPipelineParametersForExecution",
            "sagemaker:listPipelines",
            "sagemaker:listProcessingJobs",
            "sagemaker:listProjects",
            "sagemaker:listSpaces",
```

```
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:getEnabledStandards",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
```

```
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:describeActiveReceiptRuleSet",
```

```
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
```

```
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
```

```
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
```

```
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocuments",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
```

```
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeApplication",
        "sso:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
```

```
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
```

```
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
```

```
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
```

```
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
```

```
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
```

```
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSystemsManagerAccountDiscoveryServicePolicy

`AWSSystemsManagerAccountDiscoveryServicePolicy`는 AWS 관리형 정책으로, AWS Systems Manager(SSM)에 AWS 계정 정보를 검색할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 10월 24일, 17:21 UTC
- 편집된 시간: 2022년 10월 17일, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy는 AWS 관리형 정책으로, AWS Systems Manager 변경 관리 프레임워크에서 관리하거나 사용하는 AWS 리소스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 7일, 22:21 UTC
- 편집된 시간: 2020년 12월 7일, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSystemsManagerForSAPFullAccess

`AWSSystemsManagerForSAPFullAccess`는 AWS 관리형 정책으로, SAP 서비스에 대한 AWS Systems Manager에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSystemsManagerForSAPFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 17일, 02:11 UTC

- 편집된 시간: 2022년 11월 18일, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSystemsManagerForSAPReadOnlyAccess

`AWSSystemsManagerForSAPReadOnlyAccess`는 AWS 관리형 정책으로, SAP 서비스에 대한 AWS Systems Manager에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSSystemsManagerForSAPReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 17일, 02:11 UTC
- 편집된 시간: 2022년 11월 17일, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSSystemsManagerOpsDataSyncServiceRolePolicy

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`는 AWS 관리형 정책으로, OpsData 관련 작업을 관리하기 위한 SSM Explorer의 IAM 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 4월 26일, 20:42 UTC
- 편집된 시간: 2023년 6월 28일, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "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
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy는 AWS 관리형 정책으로, 이 정책은 AWS Portal Asset Server에 정상 작동에 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAssetServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:18 UTC
- 편집된 시간: 2020년 5월 27일, 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxAWSPortalAdminPolicy

`AWSThinkboxAWSPortalAdminPolicy`다음과 같은 AWS 관리형 정책입니다. 이 정책은 AWS Thinkbox의 Deadline 소프트웨어에 AWS 포털 관리에 필요한 여러 AWS 서비스에 대한 전체 액세스 권한을 부여합니다. 여기에는 여러 EC2 리소스 유형에 대한 임의의 태그를 생성할 수 있는 액세스가 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSThinkboxAWSPortalAdminPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2020년 5월 27일, 19:41 UTC
- 편집 시간: 2024년 2월 23일 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
```

```
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
```

```
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
```

```
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
```

```
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy는 AWS 관리형 정책으로, 이 정책은 AWS Portal Gateway 머신에 정상 작동에 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxAWSPortalGatewayPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:05 UTC
- 편집된 시간: 2020년 6월 30일, 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxAWSPortalWorkerPolicy

`AWSThinkboxAWSPortalWorkerPolicy`는 AWS 관리형 정책으로, 이 정책은 AWS Portal의 Deadline Workers에 정상 작동에 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSThinkboxAWSPortalWorkerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:15 UTC

- 편집된 시간: 2020년 12월 7일, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxDeadlineResourceTrackerAccessPolicy

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`는 AWS 관리형 정책으로, AWS Thinkbox의 Deadline Resource Tracker 운영에 필요한 권한을 부여합니다. 여기에는 DeleteFleets 및 CancelSpotFleetRequests를 포함한 일부 EC2 작업에 대한 전체 액세스 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSThinkboxDeadlineResourceTrackerAccessPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:25 UTC
- 편집된 시간: 2020년 5월 27일, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicy는 AWS 관리형 정책으로, AWS Thinkbox의 Deadline Resource Tracker를 생성, 삭제 및 관리하는 데 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineResourceTrackerAdminPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:29 UTC
- 편집된 시간: 2022년 6월 22일, 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
```

```
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`는 AWS 관리형 정책으로, AWS Thinkbox의 Thinkbox's Deadline Spot Event Plugin에 필요한 권한을 부여합니다. 여기에는 스팟 플릿을 요청, 수정 및 취소할 수 있는 권한과 제한된 PassRole 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSThinkboxDeadlineSpotEventPluginAdminPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:38 UTC
- 편집된 시간: 2020년 5월 27일, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy는 AWS 관리형 정책으로, AWS Thinkbox Deadline Spot Event Plugin Worker 소프트웨어를 실행하는 EC2 인스턴스에 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSThinkboxDeadlineSpotEventPluginWorkerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 27일, 19:35 UTC
- 편집된 시간: 2020년 12월 7일, 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTransferConsoleFullAccess

`AWSTransferConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Transfer에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSTransferConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 14일, 19:33 UTC
- 편집된 시간: 2020년 12월 14일, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTransferFullAccess

AWSTransferFullAccess는 AWS 관리형 정책으로, AWS Transfer Service에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 14일, 19:37 UTC
- 편집된 시간: 2020년 12월 14일, 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTransferLoggingAccess

`AWSTransferLoggingAccess`는 AWS 관리형 정책으로, AWS Transfer에 로그 스트림 및 그룹을 생성하고 계정에 로그 이벤트를 추가할 수 있는 전체 권한을 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSTransferLoggingAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 1월 14일, 15:32 UTC
- 편집된 시간: 2019년 1월 14일, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTransferReadOnlyAccess

`AWSTransferReadOnlyAccess`는 AWS 관리형 정책으로, AWS Transfer 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTransferReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 27일, 17:54 UTC
- 편집된 시간: 2020년 8월 27일, 17:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTrustedAdvisorPriorityFullAccess

`AWSTrustedAdvisorPriorityFullAccess`는 AWS 관리형 정책으로, AWS Trusted Advisor Priority에 대한 전체 액세스를 제공합니다. 또한 이 정책을 통해 사용자는 Trusted Advisor를 AWS Organizations의 신뢰할 수 있는 서비스로 추가하고 Trusted Advisor 우선 순위에 대해 위임된 관리자 계정을 지정할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSTrustedAdvisorPriorityFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 16:08 UTC
- 편집된 시간: 2022년 8월 16일, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTrustedAdvisorPriorityReadOnlyAccess

`AWSTrustedAdvisorPriorityReadOnlyAccess`는 AWS 관리형 정책으로, AWS Trusted Advisor Priority에 대한 읽기 전용 액세스를 제공합니다. 여기에는 위임된 관리자 계정을 볼 수 있는 권한이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSTrustedAdvisorPriorityReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 16일, 16:35 UTC
- 편집된 시간: 2022년 8월 16일, 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy는 AWS 관리형 정책으로, Trusted Advisor 다중 계정 보고에 대한 서비스 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 11월 19일, 17:41 UTC
- 편집된 시간: 2023년 2월 28일, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy는 AWS 관리형 정책으로, 비용 절감, 성능 향상, AWS 환경의 보안 개선을 지원하기 위한 AWS Trusted Advisor 서비스에 대한 액세스입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 2월 22일, 21:24 UTC
- 편집 시간: 2024년 1월 18일 16:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy

정책 버전

정책 버전: v12(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
```

```
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
```

```
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "kinesis:DescribeLimits",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
```

```
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy는 AWS 관리형 정책으로, AWS User Notifications가 사용자를 대신하여 AWS 서비스를 호출할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 19일, 13:28 UTC
- 편집된 시간: 2023년 4월 19일, 13:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess는 AWS 관리형 정책으로, 권한이 있는 Vendor Insights 리소스를 보고 Vendor Insights 구독을 관리할 수 있는 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsAssessorFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2022년 12월 1일, 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly는 AWS 관리형 정책으로, 권한이 있는 Vendor Insights 리소스를 볼 수 있는 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsAssessorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2022년 12월 1일, 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVendorInsightsVendorFullAccess

`AWSVendorInsightsVendorFullAccess`는 AWS 관리형 정책으로, Vendor Insights 리소스 생성 및 관리에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSVendorInsightsVendorFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2023년 10월 19일, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly는 AWS 관리형 정책으로, Vendor Insights 리소스를 볼 수 있는 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSVendorInsightsVendorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 7월 26일, 15:05 UTC
- 편집된 시간: 2022년 12월 1일, 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVpcLatticeServiceRolePolicy

`AWSVpcLatticeServiceRolePolicy`는 AWS 관리형 정책으로, VPC Lattice가 사용자를 대신하여 AWS 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 30일, 20:47 UTC
- 편집된 시간: 2022년 11월 30일, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVPCS2SVpnServiceRolePolicy

AWSVPCS2SVpnServiceRolePolicy는 AWS 관리형 정책으로, Site-to-Site VPN이 VPN 연결과 관련된 리소스를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 8월 6일, 14:13 UTC
- 편집된 시간: 2019년 8월 6일, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVPCTransitGatewayServiceRolePolicy

`AWSVPCTransitGatewayServiceRolePolicy`는 AWS 관리형 정책으로, VPC Transit Gateway가 Transit Gateway VPC Attachments에 필요한 리소스를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 26일, 16:21 UTC
- 편집된 시간: 2021년 4월 15일, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSVPCVerifiedAccessServiceRolePolicy

`AWSVPCVerifiedAccessServiceRolePolicy`는 AWS 관리형 정책으로, AWS Verified Access 서비스가 사용자를 대신하여 엔드포인트를 프로비저닝할 수 있도록 활성화하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 29일, 03:35 UTC
- 편집 시간: 2023년 11월 17일, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWAFConsoleFullAccess

`AWSWAFConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console를 통해 AWS WAF에 대한 전체 액세스를 제공합니다. 참고로 이 정책은 Amazon CloudFront 배포를 나열하고 업데이트할 수 있는 권한, AWS Elastic Load Balancing에서 로드 밸런서를 볼 수 있는 권한, Amazon API Gateway REST API 및 단계를 볼 수 있는 권한, Amazon CloudWatch 지표를 나열하고 볼 수 있는 권한, 계정 내에서 활성화된 리전을 볼 수 있는 권한도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSWAFConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 6일, 18:38 UTC
- 편집된 시간: 2023년 6월 5일, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:SetWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:SetWebACL",
        "appsync:ListGraphqlApis",
        "appsync:SetWebACL",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "s3:ListAllMyBuckets",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:ListUserPools",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Action" : [
        "logs:CreateLogDelivery",
```

```
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWAFConsoleReadOnlyAccess

AWSWAFConsoleReadOnlyAccess는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS WAF에 대한 읽기 전용 액세스를 제공합니다. 참고로 이 정책은 Amazon CloudFront 배포를 나열할 수 있는 권한, AWS Elastic Load Balancing에서 로드 밸런서를 볼 수 있는 권한, Amazon API Gateway REST API 및 단계를 볼 수 있는 권한, Amazon CloudWatch 지표를 나열하고 볼 수 있는 권한, 계정 내에서 활성화된 리전을 볼 수 있는 권한도 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFConsoleReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 6일, 18:43 UTC
- 편집된 시간: 2023년 6월 5일, 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "apigateway:GET",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "appsync:ListGraphqlApis",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWAFFullAccess

`AWSWAFFullAccess`는 AWS 관리형 정책으로, AWS WAF 작업에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSWAFFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 6일, 20:44 UTC
- 편집된 시간: 2023년 6월 5일, 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*",
        "wafv2:*",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "appsync:SetWebACL",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
```

```
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWAFReadOnlyAccess

`AWSWAFReadOnlyAccess`는 AWS 관리형 정책으로, AWS WAF 작업에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSWAFReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 10월 6일, 20:43 UTC
- 편집된 시간: 2023년 6월 5일, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy는 AWS 관리형 정책으로, WellArchitected가 고객을 대신하여 WellArchitected 리소스와 관련된 AWS 서비스 및 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 4월 26일, 18:36 UTC
- 편집된 시간: 2023년 4월 26일, 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWellArchitectedOrganizationsServiceRolePolicy

`AWSWellArchitectedOrganizationsServiceRolePolicy`는 AWS 관리형 정책으로, Well-Architected가 사용자를 대신하여 Organizations에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 6월 23일, 17:15 UTC
- 편집된 시간: 2022년 7월 25일, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSWickrFullAccess

AWSWickrFullAccess는 AWS 관리형 정책으로, 이 정책은 AWS Management Console의 Wickr 관리 기능도 포함하여 Wickr 서비스에 대한 전체 관리 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSWickrFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2022년 11월 27일, 20:36 UTC
- 편집된 시간: 2022년 11월 27일, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSXrayCrossAccountSharingConfiguration

`AWSXrayCrossAccountSharingConfiguration`는 AWS 관리형 정책으로, Observability Access Manager 링크를 관리하고 X-Ray 추적 공유를 설정하는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayCrossAccountSharingConfiguration를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:46 UTC
- 편집된 시간: 2022년 11월 27일, 13:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSXRayDaemonWriteAccess

`AWSXRayDaemonWriteAccess`는 다음과 같은 AWS 관리형 정책입니다. AWS X-Ray 데몬이 원시 추적 세그먼트 데이터를 서비스의 API로 전달하고 X-Ray SDK에서 사용할 샘플링 데이터 (규칙, 대상 등)를 검색할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `AWSXRayDaemonWriteAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2018년 8월 28일, 23:00 UTC
- 편집 시간: 2024년 2월 13일 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSXrayFullAccess

AWSXrayFullAccess는 AWS 관리형 정책으로, AWS X-Ray 전체 액세스 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:30 UTC
- 편집된 시간: 2016년 12월 1일, 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSXrayReadOnlyAccess

`AWSXrayReadOnlyAccess`는 다음과 같은 AWS 관리형 정책입니다. AWS X-Ray 읽기 전용 관리형 정책

이 정책 사용

사용자, 그룹 및 역할에 `AWSXrayReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:27 UTC
- 편집 시간: 2024년 2월 14일 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

AWSXrayWriteOnlyAccess

`AWSXrayWriteOnlyAccess`는 AWS 관리형 정책으로, AWS X-Ray 쓰기 전용 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 AWSXrayWriteOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 1일, 18:19 UTC
- 편집된 시간: 2018년 8월 28일, 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

AWSZonalAutoshiftPracticeRunSLRPolicy

`AWSZonalAutoshiftPracticeRunSLRPolicy`ARC 구역 교대 연습 실행에 대한 관리 액세스 권한과 연습 실행을 모니터링하기 위한 CloudWatch 경보 상태에 대한 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 29일 17:34 UTC
- 편집 시간: 2023년 11월 29일 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

BatchServiceRolePolicy

BatchServiceRolePolicy는 AWS 관리형 정책으로, Amazon EC2 및 Amazon ECS 리소스를 포함한 필수 리소스를 관리하기 위해 AWS Batch 서비스에 대한 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 3월 10일, 06:55 UTC
- 편집 시간: 2023년 12월 5일 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Billing

`Billing`은 AWS 관리형 정책으로, 청구 및 비용 관리에 대한 권한을 부여합니다. 여기에는 계정 사용량 보기, 예산 및 결제 방법 보기 및 수정이 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `Billing`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:33 UTC
- 편집 시간: 2024년 1월 17일 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:UpdateBillingPreferences",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
```

```
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
```

```
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CertificateManagerServiceRolePolicy

`CertificateManagerServiceRolePolicy`는 AWS 관리형 정책으로, Amazon Certificate Manager 서비스 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 6월 25일, 17:56 UTC
- 편집된 시간: 2020년 6월 25일, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ClientVPNServiceConnectionsRolePolicy

`ClientVPNServiceConnectionsRolePolicy`는 AWS 관리형 정책으로, Client VPN 엔드포인트 연결을 관리할 수 있도록 AWS Client VPN을 활성화하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 12일, 19:48 UTC
- 편집된 시간: 2020년 8월 12일, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ClientVPNServiceRolePolicy

`ClientVPNServiceRolePolicy`는 AWS 관리형 정책으로, Client VPN 엔드포인트를 관리할 수 있도록 AWS Client VPN을 활성화하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 12월 10일, 21:20 UTC
- 편집된 시간: 2020년 8월 12일, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy는 AWS 관리형 정책으로, CloudFormation StackSets(조직 마스터 계정)에 대한 서비스 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 10일, 00:20 UTC
- 편집된 시간: 2019년 12월 10일, 00:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudFormationStackSetsOrgMemberServiceRolePolicy

`CloudFormationStackSetsOrgMemberServiceRolePolicy`는 AWS 관리형 정책으로, CloudFormation StackSets(조직 멤버 계정)에 대한 서비스 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 9일, 23:52 UTC
- 편집된 시간: 2019년 12월 9일, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudFrontFullAccess

`CloudFrontFullAccess` CloudFront 콘솔에 대한 전체 액세스 권한과 를 통해 Amazon S3 버킷을 나열할 수 있는 기능을 제공하는 AWS관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `CloudFrontFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 1월 4일 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
```

```
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudFrontReadOnlyAccess

`CloudFrontReadOnlyAccess`는 를 통해 CloudFront 배포 구성 정보 및 목록 배포에 대한 액세스를 제공하는 AWS관리형 정책입니다. AWS Management Console

이 정책 사용

사용자, 그룹 및 역할에 `CloudFrontReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 1월 4일 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
```

```
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudHSMServiceRolePolicy

`CloudHSMServiceRolePolicy`는 AWS 관리형 정책으로, CloudHSM에서 사용하거나 관리하는 AWS 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 6일, 19:12 UTC
- 편집된 시간: 2017년 11월 6일, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudSearchFullAccess

`CloudSearchFullAccess`는 AWS 관리형 정책으로, Amazon CloudSearch 구성 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudSearchFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudSearchReadOnlyAccess

CloudSearchReadOnlyAccess는 AWS 관리형 정책으로, Amazon CloudSearch 구성 서비스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudSearchReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2015년 2월 6일, 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudTrailServiceRolePolicy

`CloudTrailServiceRolePolicy`다음과 같은 AWS관리형 정책입니다. 권한 정책 CloudTrail ServiceLinkedRole

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 10월 24일, 21:21 UTC
- 편집 시간: 2023년 11월 27일, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatch-CrossAccountAccess

`CloudWatch-CrossAccountAccess`는 AWS 관리형 정책으로, CloudWatch가 현재 계정을 대신하여 원격 계정에서 CloudWatch-CrossAccountSharing 역할을 맡아 계정 간, 리전 간 데이터를 표시할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 7월 23일, 09:59 UTC
- 편집된 시간: 2019년 7월 23일, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchActionsEC2Access

CloudWatchActionsEC2Access는 AWS 관리형 정책으로, CloudWatch 경보 및 지표와 EC2 메타데이터에 대한 읽기 전용 액세스를 제공합니다. EC2 인스턴스를 중지, 종료 및 재부팅할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchActionsEC2Access를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 7일, 00:00 UTC
- 편집된 시간: 2015년 7월 7일, 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchAgentAdminPolicy

`CloudWatchAgentAdminPolicy`는 다음과 같은 AWS관리형 정책입니다 AmazonCloudWatchAgent. 사용하려면 전체 권한이 필요합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchAgentAdminPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 00:52 UTC
- 편집 시간: 2024년 2월 5일 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy다음과 같은 AWS관리형 정책입니다. AmazonCloudWatchAgent 서버에서 사용하는 데 필요한 권한

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchAgentServerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 3월 7일, 01:06 UTC
- 편집 시간: 2024년 2월 6일 16:37 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchApplicationInsightsFullAccess

`CloudWatchApplicationInsightsFullAccess`는 AWS 관리형 정책으로, CloudWatch Application Insights 및 필수 종속성에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchApplicationInsightsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 24일, 18:44 UTC
- 편집된 시간: 2022년 1월 25일, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchApplicationInsightsReadOnlyAccess

CloudWatchApplicationInsightsReadOnlyAccess는 AWS 관리형 정책으로, CloudWatch Application Insights에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchApplicationInsightsReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 24일, 18:48 UTC
- 편집된 시간: 2020년 11월 24일, 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudwatchApplicationInsightsServiceLinkedRolePolicy

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Cloudwatch Application Insights 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 12월 1일, 16:22 UTC
- 편집된 시간: 2023년 5월 11일, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

정책 버전

정책 버전: v24(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
```

```
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
```

```
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
```

```
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchApplicationSignalsServiceRolePolicy

`CloudWatchApplicationSignalsServiceRolePolicy`는 다음과 같은 AWS 관리형 정책입니다. 정책은 CloudWatch 애플리케이션 시그널에 다른 관련 AWS 서비스로부터 모니터링 및 태깅 데이터를 수집할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 9일, 18:09 UTC
- 편집 시간: 2024년 3월 7일 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

CloudWatchAutomaticDashboardsAccess

`CloudWatchAutomaticDashboardsAccess`는 AWS 관리형 정책으로, Lambda 함수와 같은 객체의 콘텐츠를 포함하여 CloudWatch 자동 대시보드를 표시하는 데 사용되는 비 CloudWatch API에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchAutomaticDashboardsAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 23일, 10:01 UTC
- 편집된 시간: 2021년 4월 20일, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchCrossAccountSharingConfiguration

`CloudWatchCrossAccountSharingConfiguration`는 AWS 관리형 정책으로, Observability Access Manager 링크를 관리하고 CloudWatch 리소스 공유를 설정하는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchCrossAccountSharingConfiguration`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 14:01 UTC
- 편집된 시간: 2022년 11월 27일, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
      ]
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchEventsBuiltInTargetExecutionAccess

`CloudWatchEventsBuiltInTargetExecutionAccess`는 AWS 관리형 정책으로, Amazon CloudWatch Events에 내장된 대상이 사용자를 대신하여 EC2 작업을 수행하도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchEventsBuiltInTargetExecutionAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 14일, 18:35 UTC
- 편집된 시간: 2016년 1월 14일, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchEventsFullAccess

`CloudWatchEventsFullAccess`는 AWS 관리형 정책으로, Amazon CloudWatch Events에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchEventsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2016년 1월 14일, 18:37 UTC
- 편집된 시간: 2022년 12월 1일, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchEventsInvocationAccess

`CloudWatchEventsInvocationAccess`는 AWS 관리형 정책으로, Amazon CloudWatch Events가 사용자 계정의 AWS Kinesis Streams에 있는 스트림으로 이벤트를 릴레이할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchEventsInvocationAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2016년 1월 14일, 18:36 UTC
- 편집된 시간: 2016년 1월 14일, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchEventsReadOnlyAccess

`CloudWatchEventsReadOnlyAccess`는 AWS 관리형 정책으로, Amazon CloudWatch Events에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchEventsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책

- 생성 시간: 2016년 1월 14일, 18:27 UTC
- 편집된 시간: 2022년 12월 1일, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchEventsServiceRolePolicy

`CloudWatchEventsServiceRolePolicy`는 AWS 관리형 정책으로, AWS CloudWatch가 사용자를 대신하여 경보 및 이벤트를 통해 구성된 작업을 실행하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 17일, 00:42 UTC
- 편집된 시간: 2017년 11월 17일, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchFullAccess

`CloudWatchFullAccess`는 AWS 관리형 정책으로, CloudWatch에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2022년 11월 27일, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchFullAccessV2

CloudWatchFullAccessV2에 대한 전체 액세스를 제공하는 AWS관리형 CloudWatch 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchFullAccessV2를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 8월 1일, 11:32 UTC
- 편집 시간: 2023년 12월 5일 19:36 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
```

```
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchInternetMonitorServiceRolePolicy

`CloudWatchInternetMonitorServiceRolePolicy`는 AWS 관리형 정책으로, Internet Monitor가 사용자를 대신하여 EC2, Workspaces, CloudFront 리소스 및 기타 필수 서비스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 27일, 17:46 UTC
- 편집된 시간: 2023년 7월 20일, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy는 AWS 관리형 정책으로, Lambda Insights 확장 프로그램에 필요한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 CloudWatchLambdaInsightsExecutionRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 10월 7일, 19:27 UTC
- 편집된 시간: 2020년 10월 7일, 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchLogsCrossAccountSharingConfiguration

`CloudWatchLogsCrossAccountSharingConfiguration`는 AWS 관리형 정책으로, Observability Access Manager 링크를 관리하고 CloudWatch Logs 리소스 공유를 설정하는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchLogsCrossAccountSharingConfiguration`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:55 UTC
- 편집된 시간: 2022년 11월 27일, 13:55 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchLogsFullAccess

`CloudWatchLogsFullAccess` CloudWatch 로그에 대한 전체 액세스 권한을 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchLogsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 11월 26일 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchLogsReadOnlyAccess

`CloudWatchLogsReadOnlyAccess` CloudWatch Log에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchLogsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 11월 26일 18:11 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchNetworkMonitorServiceRolePolicy

`CloudWatchNetworkMonitorServiceRolePolicy` CloudWatch Network Monitor가 사용자를 대신하여 EC2 및 VPC 리소스에 액세스 및 관리하고, 데이터를 게시하고, 다른 필수 서비스에 액세스할 CloudWatch 수 있도록 하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 12월 21일 18:53 UTC
- 편집 시간: 2023년 12월 21일 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchReadOnlyAccess

`CloudWatchReadOnlyAccess`읽기 전용 액세스를 제공하는 AWS관리형 CloudWatch 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집 시간: 2023년 12월 5일 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchSyntheticsFullAccess

`CloudWatchSyntheticsFullAccess`는 AWS 관리형 정책으로, CloudWatch Synthetics에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchSyntheticsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 25일, 17:39 UTC
- 편집된 시간: 2022년 5월 6일, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

정책 버전

정책 버전: v9(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CloudWatchSyntheticsReadOnlyAccess

`CloudWatchSyntheticsReadOnlyAccess`는 AWS 관리형 정책으로, CloudWatch Synthetics에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CloudWatchSyntheticsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 11월 25일, 17:45 UTC
- 편집된 시간: 2020년 3월 6일, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComprehendDataAccessRolePolicy

`ComprehendDataAccessRolePolicy`는 AWS 관리형 정책으로, 데이터 액세스를 위해 S3 리소스에 대한 액세스를 허용하는 AWS Comprehend 서비스 역할에 대한 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ComprehendDataAccessRolePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2019년 3월 6일, 22:28 UTC
- 편집된 시간: 2019년 3월 6일, 22:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComprehendFullAccess

`ComprehendFullAccess`는 AWS 관리형 정책으로, Amazon Comprehend에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ComprehendFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:08 UTC
- 편집된 시간: 2017년 12월 5일, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComprehendMedicalFullAccess

`ComprehendMedicalFullAccess`는 AWS 관리형 정책으로, Amazon Comprehend Medical에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ComprehendMedicalFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 17:55 UTC
- 편집된 시간: 2018년 11월 27일, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComprehendReadOnly

`ComprehendReadOnly`는 AWS 관리형 정책으로, Amazon Comprehend에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ComprehendReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:10 UTC
- 편집된 시간: 2022년 4월 26일, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComputeOptimizerReadOnlyAccess

`ComputeOptimizerReadOnlyAccess`는 AWS 관리형 정책으로, ComputeOptimizer에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 ComputeOptimizerReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 3월 7일, 00:11 UTC
- 편집된 시간: 2023년 8월 28일, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
```

```
        "compute-optimizer:GetLicenseRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ComputeOptimizerServiceRolePolicy

`ComputeOptimizerServiceRolePolicy`는 AWS 관리형 정책으로, ComputeOptimizer가 사용자를 대신하여 AWS 서비스를 호출하고 워크로드 세부 정보를 수집할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 12월 3일, 08:45 UTC
- 편집된 시간: 2022년 6월 13일, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ConfigConformsServiceRolePolicy

ConfigConformsServiceRolePolicy는 AWS 관리형 정책으로, AWSConfig에서 적합성 팩을 생성하는 데 필요한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 7월 25일, 21:38 UTC
- 편집된 시간: 2023년 1월 12일, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CostOptimizationHubAdminAccess

`CostOptimizationHubAdminAccess`다음과 같은 AWS관리형 정책입니다. 이 관리형 정책은 관리자에게 비용 최적화 허브에 대한 액세스 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CostOptimizationHubAdminAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 12월 19일 00:03 UTC
- 편집 시간: 2023년 12월 19일 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CostOptimizationHubReadOnlyAccess

`CostOptimizationHubReadOnlyAccess`는 다음과 같은 AWS관리형 정책입니다. 이 관리형 정책은 비용 최적화 허브에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `CostOptimizationHubReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 13일 18:04 UTC
- 편집 시간: 2023년 12월 13일 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CostOptimizationHubServiceRolePolicy

`CostOptimizationHubServiceRolePolicy`Cost Optimization Hub가 조직 정보를 검색하고 최적화 관련 데이터 및 메타데이터를 수집할 수 있도록 하는 AWS관리형 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 11월 26일, 08:03 UTC
- 편집 시간: 2023년 11월 26일, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

CustomerProfilesServiceLinkedRolePolicy

`CustomerProfilesServiceLinkedRolePolicy`는 AWS 관리형 정책으로, Amazon Connect Customer Profiles이 사용자를 대신하여 AWS 서비스 및 리소스에 액세스할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 3월 7일, 22:56 UTC
- 편집된 시간: 2023년 3월 7일, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DatabaseAdministrator

DatabaseAdministrator는 AWS 관리형 정책으로, AWS 데이터베이스 서비스를 설정하고 구성하는 데 필요한 AWS 서비스 및 작업에 대한 전체 액세스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 DatabaseAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:25 UTC
- 편집된 시간: 2019년 1월 8일, 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DataScientist

`DataScientist`는 AWS 관리형 정책으로, AWS 데이터 분석 서비스에 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `DataScientist`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:28 UTC
- 편집된 시간: 2019년 12월 3일, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DAXServiceRolePolicy

DAXServiceRolePolicy는 AWS 관리형 정책으로, 이 정책은 DAX가 고객을 대신하여 네트워크 인터페이스, 보안 그룹, 서브넷 및 VPC를 생성하고 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 5일, 17:51 UTC
- 편집된 시간: 2018년 3월 5일, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy는 AWS 관리형 정책으로, Amazon DynamoDB용 Amazon CloudWatch Contributor Insights를 지원하는 데 필요한 권한입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 15일, 21:13 UTC
- 편집된 시간: 2019년 11월 15일, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy는 AWS 관리형 정책으로, KinesisDataStreams에 대한 AWS DynamoDB 액세스를 제공합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 12일, 00:43 UTC
- 편집된 시간: 2020년 11월 12일, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy는 AWS 관리형 정책으로, DynamoDB에서 리전 간 데이터 복제를 위해 필요한 권한입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 11월 9일, 23:55 UTC
- 편집 시간: 2024년 1월 8일 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy는 AWS 관리형 정책으로, ec2fastlaunch가 고객 계정에서 사전 프로비저닝된 스냅샷을 준비 및 관리하고 관련 지표를 게시할 수 있도록 권한을 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 1월 10일, 13:08 UTC
- 편집된 시간: 2022년 1월 10일, 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2FleetTimeShiftableServiceRolePolicy

`EC2FleetTimeShiftableServiceRolePolicy`는 AWS 관리형 정책으로, EC2 Fleet에 향후 인스턴스를 시작할 수 있는 권한을 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책

- 생성 시간: 2019년 12월 23일, 19:47 UTC
- 편집된 시간: 2019년 12월 23일, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Ec2ImageBuilderCrossAccountDistributionAccess

`Ec2ImageBuilderCrossAccountDistributionAccess`는 AWS 관리형 정책으로, EC2 Image Builder에서 교차 계정 분배를 수행하는 데 필요한 권한입니다.

이 정책 사용

사용자, 그룹 및 역할에 Ec2ImageBuilderCrossAccountDistributionAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 30일, 19:22 UTC
- 편집된 시간: 2020년 9월 30일, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2ImageBuilderLifecycleExecutionPolicy

`EC2ImageBuilderLifecycleExecutionPolicy`는 다음과 같은 AWS관리형 정책입니다. EC2 ImageBuilderLifecycleExecutionPolicy 정책은 Image Builder에 Image Builder 이미지 리소스 및 기본 리소스 (AMI, 스냅샷) 를 사용 중단하거나 삭제하는 등의 작업을 수행할 수 있는 권한을 부여하여 이미지 수명 주기 관리 작업에 대한 자동화된 규칙을 지원합니다.

이 정책 사용

사용자, 그룹 및 역할에 `EC2ImageBuilderLifecycleExecutionPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 11월 16일 23:23 UTC
- 편집 시간: 2023년 11월 16일, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2InstanceConnect

EC2InstanceConnect는 AWS 관리형 정책으로, 고객이 EC2 Instance Connect를 호출하여 EC2 인스턴스에 임시 키를 게시하고 ssh 또는 EC2 Instance Connect CLI를 통해 연결할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 EC2InstanceConnect를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 27일, 18:53 UTC
- 편집된 시간: 2019년 6월 27일, 18:53 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceConnect

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
```

```
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Ec2InstanceConnectEndpoint

`Ec2InstanceConnectEndpoint`는 AWS 관리형 정책으로, 고객이 생성한 EC2 Instance Connect 엔드포인트를 관리하기 위한 EC2 Instance Connect 엔드포인트 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 24일, 20:19 UTC
- 편집된 시간: 2023년 1월 24일, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
          ]
        }
      }
    }
```

```
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2InstanceProfileForImageBuilder

`EC2InstanceProfileForImageBuilder`는 AWS 관리형 정책으로, Image Builder 서비스를 위한 EC2 Instance 프로파일인 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `EC2InstanceProfileForImageBuilder`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 1일, 19:08 UTC
- 편집된 시간: 2020년 8월 27일, 16:40 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EC2InstanceProfileForImageBuilderECRContainerBuilds

`EC2InstanceProfileForImageBuilderECRContainerBuilds`는 AWS 관리형 정책으로, EC2 Image Builder를 통해 컨테이너 이미지를 빌드하기 위한 EC2 Instance 프로파일입니다. 이 정책은 사용자에게 ECR 이미지를 업로드할 수 있는 광범위한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `EC2InstanceProfileForImageBuilderECRContainerBuilds`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 12월 11일, 19:48 UTC
- 편집된 시간: 2020년 12월 11일, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ECRReplicationServiceRolePolicy

`ECRReplicationServiceRolePolicy`는 AWS 관리형 정책으로, ECR Replication에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 4일, 22:11 UTC
- 편집된 시간: 2020년 12월 4일, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElastiCacheServiceRolePolicy

`ElastiCacheServiceRolePolicy`는 다음과 같은 AWS관리형 정책입니다. 이 정책을 통해 ElastiCache 캐시 관리에 필요한 AWS 리소스를 사용자 대신 관리할 수 있습니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 12월 7일, 17:50 UTC
- 편집 시간: 2023년 11월 28일 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "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/*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElasticLoadBalancingFullAccess

`ElasticLoadBalancingFullAccess`는 AWS 관리형 정책으로, Amazon ElasticLoadBalancing에 대한 전체 액세스를 제공하고 ElasticLoadBalancing 기능을 제공하는 데 필요한 다른 서비스에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElasticLoadBalancingFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 9월 20일, 20:42 UTC
- 편집된 시간: 2022년 11월 29일, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeVpcPeeringConnections",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElasticLoadBalancingReadOnly

`ElasticLoadBalancingReadOnly`Amazon ElasticLoadBalancing 및 종속 서비스에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElasticLoadBalancingReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 9월 20일, 20:17 UTC
- 편집 시간: 2023년 11월 26일 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalActivationsDownloadSoftwareAccess

`ElementalActivationsDownloadSoftwareAccess`는 AWS 관리형 정책으로, 구매 자산을 보고 관련 소프트웨어 및 킥스타트 파일을 다운로드할 수 있는 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalActivationsDownloadSoftwareAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 9월 8일, 17:26 UTC
- 편집된 시간: 2020년 9월 8일, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalActivationsFullAccess

`ElementalActivationsFullAccess`는 AWS 관리형 정책으로, Elemental Appliance 및 Software 구매 자산을 보고 조치를 취할 수 있는 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalActivationsFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 6월 4일, 21:00 UTC
- 편집된 시간: 2020년 6월 4일, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalActivationsGenerateLicenses

`ElementalActivationsGenerateLicenses`는 AWS 관리형 정책으로, 구매 자산을 보고 보류 중인 활성화에 대한 소프트웨어 라이선스를 생성할 수 있는 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalActivationsGenerateLicenses`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 28일, 18:28 UTC
- 편집된 시간: 2020년 8월 28일, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalActivationsReadOnlyAccess

`ElementalActivationsReadOnlyAccess`는 AWS 관리형 정책으로, 사용자 AWS 계정과 연관된 구매 자산의 세부 목록에 대한 읽기 전용 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalActivationsReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 8월 28일, 16:51 UTC
- 편집된 시간: 2020년 8월 28일, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalAppliancesSoftwareFullAccess

`ElementalAppliancesSoftwareFullAccess`는 AWS 관리형 정책으로, Elemental Appliance 및 Software 견적 및 주문을 보고 조치를 취할 수 있는 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalAppliancesSoftwareFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 7월 31일, 16:28 UTC
- 편집된 시간: 2021년 2월 5일, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalAppliancesSoftwareReadOnlyAccess

`ElementalAppliancesSoftwareReadOnlyAccess`는 AWS 관리형 정책으로, Elemental Appliance 및 Software 견적 및 주문을 볼 수 있는 읽기 전용 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalAppliancesSoftwareReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 1일, 22:31 UTC
- 편집된 시간: 2020년 4월 1일, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ElementalSupportCenterFullAccess

`ElementalSupportCenterFullAccess`는 AWS 관리형 정책으로, Elemental Appliance 및 Software 지원 사례와 제품 지원 콘텐츠를 보고 조치를 취할 수 있는 전체 액세스입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ElementalSupportCenterFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 11월 25일, 18:08 UTC
- 편집된 시간: 2021년 2월 5일, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL는 AWS 관리형 정책으로, Amazon EMR용 WAL 서비스가 클러스터의 상태를 찾고 반환할 수 있도록 허용하는 읽기 전용 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 6월 15일, 23:30 UTC
- 편집된 시간: 2023년 6월 15일, 23:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

FMSServiceRolePolicy

FMSServiceRolePolicy는 AWS 관리형 정책으로, FM 서비스 연결 역할이 고객 AWS Organization 계정 내의 FM 관리 리소스에 대해 FM 관련 작업을 수행할 수 있도록 허용하는 액세스 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 3월 28일, 23:01 UTC
- 편집된 시간: 2023년 4월 21일, 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

정책 버전

정책 버전: v28(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
```

```
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
```

```
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "ram",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
```

```
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:PutResourcePolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
```

```
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess는 AWS 관리형 정책으로, Amazon FSx가 Amazon S3 액세스에 대한 서비스 연결 역할을 삭제할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 28일, 10:40 UTC
- 편집된 시간: 2018년 11월 28일, 10:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GameLiftGameServerGroupPolicy

`GameLiftGameServerGroupPolicy`는 AWS 관리형 정책으로, Gamelift GameServerGroups가 고객 리소스를 관리할 수 있도록 허용하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `GameLiftGameServerGroupPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 4월 3일, 23:12 UTC
- 편집된 시간: 2020년 5월 13일, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GlobalAcceleratorFullAccess

`GlobalAcceleratorFullAccess`는 AWS 관리형 정책으로, GlobalAccelerator 사용자에게 모든 API에 대한 전체 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `GlobalAcceleratorFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 02:44 UTC

- 편집된 시간: 2020년 12월 4일, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GlobalAcceleratorReadOnlyAccess

`GlobalAcceleratorReadOnlyAccess`는 AWS 관리형 정책으로, GlobalAccelerator 사용자에게 읽기 전용 API에 대한 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `GlobalAcceleratorReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 02:41 UTC
- 편집된 시간: 2018년 11월 27일, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GreengrassOTAUpdateArtifactAccess

`GreengrassOTAUpdateArtifactAccess`는 AWS 관리형 정책으로, 모든 Greengrass 리전의 Greengrass OTA 업데이트 아티팩트에 대한 읽기 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `GreengrassOTAUpdateArtifactAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책

- 생성 시간: 2017년 11월 29일, 18:11 UTC
- 편집된 시간: 2018년 12월 18일, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GroundTruthSyntheticConsoleFullAccess

`GroundTruthSyntheticConsoleFullAccess`는 AWS 관리형 정책으로, 이 정책은 ageMaker Ground Truth Synthetic Console의 모든 기능을 사용하는 데 필요한 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `GroundTruthSyntheticConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 25일, 15:58 UTC
- 편집된 시간: 2022년 8월 25일, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

GroundTruthSyntheticConsoleReadOnlyAccess

`GroundTruthSyntheticConsoleReadOnlyAccess`는 AWS 관리형 정책으로, 이 정책은 AWS Management Console을 통해 SageMaker Ground Truth Synthetic에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `GroundTruthSyntheticConsoleReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 8월 25일, 15:58 UTC
- 편집된 시간: 2022년 8월 25일, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Health_OrganizationsServiceRolePolicy

`Health_OrganizationsServiceRolePolicy`는 AWS 관리형 정책으로, Organizational View 기능을 활성화하기 위한 AWS Health 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 12월 16일, 13:28 UTC
- 편집 시간: 2024년 2월 6일 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMAccessAdvisorReadOnly

`IAMAccessAdvisorReadOnly`는 AWS 관리형 정책으로, 이 정책은 서비스에서 마지막으로 액세스한 정보 등 IAM 액세스 관리자가 제공하는 모든 액세스 정보에 대한 읽기 전용 액세스를 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMAccessAdvisorReadOnly를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 21일, 19:33 UTC
- 편집된 시간: 2019년 6월 21일, 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMAccessAnalyzerFullAccess

`IAMAccessAnalyzerFullAccess`는 AWS 관리형 정책으로, IAM Access Analyzer에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMAccessAnalyzerFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 2일, 17:12 UTC
- 편집된 시간: 2019년 12월 2일, 17:12 UTC

- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMAccessAnalyzerReadOnlyAccess

`IAMAccessAnalyzerReadOnlyAccess`는 AWS 관리형 정책으로, IAM Access Analyzer 리소스에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMAccessAnalyzerReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 12월 2일, 17:12 UTC
- 편집 시간: 2023년 11월 27일, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMFullAccess

`IAMFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 IAM에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2019년 6월 21일, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMReadOnlyAccess

`IAMReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 IAM에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:40 UTC
- 편집된 시간: 2018년 1월 25일, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMSelfManageServiceSpecificCredentials

`IAMSelfManageServiceSpecificCredentials`는 AWS 관리형 정책으로, IAM 사용자가 자신의 서비스별 보안 인증 정보를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMSelfManageServiceSpecificCredentials`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 12월 22일, 17:25 UTC
- 편집된 시간: 2016년 12월 22일, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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}"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMUserChangePassword

`IAMUserChangePassword`는 AWS 관리형 정책으로, IAM 사용자가 자신의 암호를 변경할 수 있는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 IAMUserChangePassword를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 11월 15일, 00:25 UTC
- 편집된 시간: 2016년 11월 15일, 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IAMUserSSHKeys

`IAMUserSSHKeys`는 AWS 관리형 정책으로, IAM 사용자가 자신의 SSH 키를 관리할 수 있는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `IAMUserSSHKeys`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 7월 9일, 17:08 UTC
- 편집된 시간: 2015년 7월 9일, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "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}"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IVSFullAccess

`IVSFullAccess`는 IVS (대화형 비디오 서비스) 에 대한 전체 액세스를 제공하고 ivs 콘솔에 완전히 액세스하는 데 필요한 종속 서비스에 대한 권한도 포함하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `IVSFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 작성 시간: 2023년 12월 13일, 21:20 UTC
- 편집 시간: 2023년 12월 13일 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

IVSReadOnlyAccess

`IVSReadOnlyAccess`IVS 저지연 및 실시간 스트리밍 API에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 IVSReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 작성 시간: 2023년 12월 5일 18:00 UTC
- 편집 시간: 2024년 2월 16일 18:03 UTC
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
```

```
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

IVSRecordToS3

`IVSRecordToS3`는 AWS 관리형 정책으로, IVS 라이브 스트림을 기록하기 위해 S3 PutObject를 수행하는 서비스 연결 역할입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 12월 5일, 00:10 UTC
- 편집된 시간: 2020년 12월 5일, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy는 AWS 관리형 정책으로, 이 정책은 Kafka Connect에 사용자를 대신하여 AWS 리소스를 관리할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 9월 7일, 13:12 UTC
- 편집된 시간: 2021년 9월 7일, 13:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

KafkaServiceRolePolicy

KafkaServiceRolePolicy는 AWS 관리형 정책으로, Kafka에 대한 IAM 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 11월 15일, 23:31 UTC
- 편집된 시간: 2023년 4월 28일, 00:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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_*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy는 AWS 관리형 정책으로, Keyspaces에서 리전 간 데이터 복제를 위해 필요한 권한입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 5월 2일, 16:15 UTC
- 편집된 시간: 2023년 5월 2일, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

LakeFormationDataAccessServiceRolePolicy

`LakeFormationDataAccessServiceRolePolicy`는 AWS 관리형 정책으로, Lake Formation 리소스에 대한 임시 데이터 액세스를 부여하는 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 20일, 20:46 UTC
- 편집 시간: 2024년 2월 6일 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

LexBotPolicy

LexBotPolicy는 AWS 관리형 정책으로, AWS Lex Bot 사용 사례 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 2월 17일, 22:18 UTC
- 편집된 시간: 2019년 11월 13일, 22:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

LexChannelPolicy

`LexChannelPolicy`는 AWS 관리형 정책으로, AWS Lex Channel 사용 사례 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2017년 2월 17일, 23:23 UTC
- 편집된 시간: 2017년 2월 17일, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

LightsailExportAccess

`LightsailExportAccess`는 AWS 관리형 정책으로, 리소스 내보내기 권한을 부여하는 AWS Lightsail 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 9월 28일, 16:35 UTC
- 편집된 시간: 2022년 1월 15일, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MediaConnectGatewayInstanceRolePolicy

`MediaConnectGatewayInstanceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 MediaConnect Gateway Instances를 MediaConnect Gateway에 등록할 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `MediaConnectGatewayInstanceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 22일, 20:43 UTC
- 편집된 시간: 2023년 3월 22일, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
```

```
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MediaPackageServiceRolePolicy

`MediaPackageServiceRolePolicy`는 AWS 관리형 정책으로, MediaPackage가 CloudWatch에 로그를 게시할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 9월 18일, 17:45 UTC
- 편집된 시간: 2020년 9월 18일, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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/*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MemoryDBServiceRolePolicy

`MemoryDBServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 MemoryDB가 사용자를 대신하여 리소스 관리에 필요한 만큼 AWS 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 8월 17일, 22:34 UTC
- 편집된 시간: 2021년 8월 18일, 23:48UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MigrationHubDMSAccessServiceRolePolicy

`MigrationHubDMSAccessServiceRolePolicy`는 AWS 관리형 정책으로, Database Migration Service가 고객의 계정에서 역할을 맡아 Migration Hub를 호출하도록 하기 위한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 17:50 UTC
- 편집된 시간: 2019년 10월 7일, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "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" : "*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MigrationHubServiceRolePolicy

`MigrationHubServiceRolePolicy`는 AWS 관리형 정책으로, Migration Hub가 사용자를 대신하여 Application Discovery Service를 호출하도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 17:22 UTC
- 편집된 시간: 2020년 8월 6일, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
```

```
  "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" : [
```

```
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MigrationHubSMSAccessServiceRolePolicy

`MigrationHubSMSAccessServiceRolePolicy`는 AWS 관리형 정책으로, Server Migration Service가 고객의 계정에서 역할을 맡아 Migration Hub를 호출하도록 하기 위한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 6월 12일, 18:30 UTC
- 편집된 시간: 2019년 10월 7일, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해

- AWS 관리형 정책을 시작하고 최소 권한으로 전환

MonitronServiceRolePolicy

MonitronServiceRolePolicy는 AWS 관리형 정책으로, 필수 고객 리소스에 대한 액세스를 부여하는 AWS Monitron 서비스 연결 역할에 대한 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 5월 2일, 19:22 UTC
- 편집된 시간: 2022년 5월 2일, 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

NeptuneConsoleFullAccess

NeptuneConsoleFullAccess는 AWS 관리형 정책으로, AWS Management Console을 사용하여 Amazon Neptune을 관리할 수 있는 전체 액세스를 제공합니다. 참고로 이 정책은 또한 계정 내의 모든 SNS 주제에 대해 게시할 수 있는 전체 액세스, Amazon EC2 인스턴스 및 VPC 구성을 생성 및 편집할 수 있는 권한, Amazon KMS에서 키를 보고 나열할 수 있는 권한, Amazon RDS에 대한 전체 액세스도 부여합니다. 자세한 내용은 https://aws.amazon.com/neptune/faqs/를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneConsoleFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 6월 19일, 21:35 UTC
- 편집 시간: 2023년 11월 30일 07:32 UTC
- ARN: arn:aws:iam::aws:policy/NeptuneConsoleFullAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

NeptuneFullAccess

`NeptuneFullAccess`는 AWS 관리형 정책으로, Amazon Neptune에 대한 전체 액세스를 제공합니다. 참고로 이 정책은 계정 내 모든 SNS 주제에 대한 게시에 대한 전체 액세스와 Amazon RDS에 대한 전체 액세스도 부여합니다. 자세한 내용은 https://aws.amazon.com/neptune/faqs/를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 `NeptuneFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 30일, 19:17 UTC
- 편집 시간: 2024년 1월 22일 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

NeptuneGraphReadOnlyAccess

`NeptuneGraphReadOnlyAccess`종속 서비스에 대한 읽기 전용 권한과 함께 모든 Amazon Neptune Analytics 리소스에 대한 읽기 전용 액세스를 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `NeptuneGraphReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 30일, 07:32 UTC
- 편집 시간: 2023년 11월 30일, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

NeptuneReadOnlyAccess

NeptuneReadOnlyAccess는 AWS 관리형 정책으로, Amazon Neptune에 대한 읽기 전용 액세스를 제공합니다. 참고로 이 정책은 Amazon RDS 리소스에 대한 액세스 권한도 부여합니다. 자세한 내용은 https://aws.amazon.com/neptune/faqs/를 참조하세요.

이 정책 사용

사용자, 그룹 및 역할에 NeptuneReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 5월 30일, 19:16 UTC
- 편집 시간: 2024년 1월 22일 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

NetworkAdministrator

NetworkAdministrator는 AWS 관리형 정책으로, AWS 네트워크 리소스를 설정하고 구성하는 데 필요한 AWS 서비스 및 작업에 대한 전체 액세스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 NetworkAdministrator를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:31 UTC
- 편집된 시간: 2021년 9월 16일, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

정책 버전

정책 버전: v11(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
```

```
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeIpv6Pools",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
```

```
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
```

```
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
```

```
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
```

```
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

OAMFullAccess

OAMFullAccess는 AWS 관리형 정책으로, CloudWatch Observability Access Manager에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 OAMFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:38 UTC
- 편집된 시간: 2022년 11월 27일, 13:38 UTC
- ARN: arn:aws:iam::aws:policy/OAMFullAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

OAMReadOnlyAccess

`OAMReadOnlyAccess`는 AWS 관리형 정책으로, CloudWatch Observability Access Manager에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `OAMReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 11월 27일, 13:29 UTC
- 편집된 시간: 2022년 11월 27일, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

PartnerCentralAccountManagementUserRoleAssociation

`PartnerCentralAccountManagementUserRoleAssociation`는 AWS 관리형 정책으로, 파트너 중앙 사용자를 IAM 역할과 연결 및 분리할 수 있는 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `PartnerCentralAccountManagementUserRoleAssociation`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 11월 10일, 02:03 UTC
- 편집된 시간: 2023년 11월 10일, 02:03 UTC

- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

PowerUserAccess

PowerUserAccess는 AWS 관리형 정책으로, AWS 서비스 및 리소스에 대한 전체 액세스를 제공하지만 사용자 및 그룹 관리는 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 PowerUserAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2023년 7월 6일, 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeOrganization",
        "account:ListRegions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`는 AWS 관리형 정책으로, QuickSight 팀이 S3 스토리지 관리 분석에서 생성한 고객 데이터에 액세스하는 데 사용하는 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `QuickSightAccessForS3StorageManagementAnalyticsReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2017년 6월 12일, 18:18 UTC
- 편집된 시간: 2019년 10월 8일, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
```

```
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

RDSCloudHsmAuthorizationRole

`RDSCloudHsmAuthorizationRole`는 AWS 관리형 정책으로, Amazon RDS 서비스 역할에 대한 기본 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `RDSCloudHsmAuthorizationRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2019년 9월 26일, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ReadOnlyAccess

`ReadOnlyAccess` AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공하는 AWS 관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집 시간: 2024년 2월 5일 오후 5시 (UTC)
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

정책 버전

정책 버전: v111(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
```

```
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "aoss:BatchGetCollection",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
```

```
            "appfabric:GetIngestion",
            "appfabric:GetIngestionDestination",
            "appfabric:ListAppAuthorizations",
            "appfabric:ListAppBundles",
            "appfabric:ListIngestionDestinations",
            "appfabric:ListIngestions",
            "appfabric:ListTagsForResource",
            "appflow:DescribeConnector",
            "appflow:DescribeConnectorEntity",
            "appflow:DescribeConnectorFields",
            "appflow:DescribeConnectorProfiles",
            "appflow:DescribeConnectors",
            "appflow:DescribeFlow",
            "appflow:DescribeFlowExecution",
            "appflow:DescribeFlowExecutionRecords",
            "appflow:DescribeFlows",
            "appflow:ListConnectorEntities",
            "appflow:ListConnectorFields",
            "appflow:ListConnectors",
            "appflow:ListFlows",
            "appflow:ListTagsForResource",
            "application-autoscaling:Describe*",
            "application-autoscaling:ListTagsForResource",
            "applicationinsights:Describe*",
            "applicationinsights:List*",
            "appmesh:Describe*",
            "appmesh:List*",
            "apprunner:DescribeAutoScalingConfiguration",
            "apprunner:DescribeCustomDomains",
            "apprunner:DescribeObservabilityConfiguration",
            "apprunner:DescribeService",
            "apprunner:DescribeVpcConnector",
            "apprunner:DescribeVpcIngressConnection",
            "apprunner:ListAutoScalingConfigurations",
            "apprunner:ListConnections",
            "apprunner:ListObservabilityConfigurations",
            "apprunner:ListOperations",
            "apprunner:ListServices",
            "apprunner:ListTagsForResource",
            "apprunner:ListVpcConnectors",
            "apprunner:ListVpcIngressConnections",
            "appstream:Describe*",
            "appstream:List*",
            "appsync:Get*",
```

```
        "appsync:List*",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
```

```
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
```

```
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
```

```
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams",
        "chatbot:ListMicrosoftTeamsUserIdentities",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
```

```
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
```

```
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
```

```
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
```

```
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
```

```
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
```

```
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
```

```
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
```

```
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
```

```
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
```

```
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
```

```
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
```

```
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
```

```
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
```

```
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
```

```
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
```

```
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
```

```
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
```

```
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
```

```
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
```

```
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
```

```
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
```

```
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
```

```
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
```

```
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
```

```
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeChannel",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:ListChannels",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
```

```
            "mediastore:GetMetricPolicy",
            "mediastore:GetObject",
            "mediastore:ListContainers",
            "mediastore:ListItems",
            "mediastore:ListTagsForResource",
            "memorydb:DescribeClusters",
            "memorydb:DescribeParameterGroups",
            "memorydb:DescribeParameters",
            "memorydb:ListTags",
            "mgh:Describe*",
            "mgh:GetHomeRegion",
            "mgh:List*",
            "mgn:DescribeJobLogItems",
            "mgn:DescribeJobs",
            "mgn:DescribeLaunchConfigurationTemplates",
            "mgn:DescribeReplicationConfigurationTemplates",
            "mgn:DescribeSourceServers",
            "mgn:DescribeVcenterClients",
            "mgn:GetLaunchConfiguration",
            "mgn:GetReplicationConfiguration",
            "mgn:ListApplications",
            "mgn:ListSourceServerActions",
            "mgn:ListTemplateActions",
            "mgn:ListWaves",
            "mobileanalytics:Get*",
            "mobiletargeting:Get*",
            "mobiletargeting:List*",
            "monitron:GetProject",
            "monitron:GetProjectAdminUser",
            "monitron:ListProjects",
            "monitron:ListTagsForResource",
            "mq:Describe*",
            "mq:List*",
            "network-firewall:DescribeFirewall",
            "network-firewall:DescribeFirewallPolicy",
            "network-firewall:DescribeLoggingConfiguration",
            "network-firewall:DescribeResourcePolicy",
            "network-firewall:DescribeRuleGroup",
            "network-firewall:DescribeRuleGroupMetadata",
            "network-firewall:DescribeTLSInspectionConfiguration",
            "network-firewall:ListFirewallPolicies",
            "network-firewall:ListFirewalls",
            "network-firewall:ListRuleGroups",
            "network-firewall:ListTagsForResource",
```

```
        "network-firewall:ListTLSInspectionConfigurations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
```

```
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
```

```
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
```

```
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
```

```
        "rds:Download*",
        "rds:List*",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAlarmRecommendations",
```

```
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
```

```
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
```

```
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
```

```
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListEngagements",
        "ssm-contacts:ListPageReceipts",
        "ssm-contacts:ListPagesByContact",
        "ssm-contacts:ListPagesByEngagement",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:GetReplicationSet",
```

```
        "ssm-incidents:GetResourcePolicies",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-incidents:ListTimelineEvents",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "sustainability:GetCarbonFootprintSummary",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
```

```
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
```

```
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
```

```
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:ListAnswers",
        "wellarchitected:ListCheckDetails",
        "wellarchitected:ListCheckSummaries",
        "wellarchitected:ListLenses",
        "wellarchitected:ListLensReviewImprovements",
        "wellarchitected:ListLensReviews",
        "wellarchitected:ListLensShares",
        "wellarchitected:ListMilestones",
        "wellarchitected:ListNotifications",
        "wellarchitected:ListProfileNotifications",
        "wellarchitected:ListProfiles",
        "wellarchitected:ListProfileShares",
        "wellarchitected:ListReviewTemplateAnswers",
        "wellarchitected:ListReviewTemplates",
        "wellarchitected:ListShareInvitations",
        "wellarchitected:ListTagsForResource",
        "wellarchitected:ListTemplateShares",
        "wellarchitected:ListWorkloads",
        "wellarchitected:ListWorkloadShares",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
```

```
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

ResourceGroupsandTagEditorFullAccess

`ResourceGroupsandTagEditorFullAccess`는 AWS 관리형 정책으로, Resource Groups 및 Tag Editor에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ResourceGroupsandTagEditorFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2023년 8월 10일, 13:29 UTC

- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ResourceGroupsandTagEditorReadOnlyAccess

ResourceGroupsandTagEditorReadOnlyAccess는 AWS 관리형 정책으로, Resource Groups 및 Tag Editor를 사용할 수 있는 액세스는 제공하지만 Tag Editor를 통한 태그 편집은 허용하지 않습니다.

이 정책 사용

사용자, 그룹 및 역할에 ResourceGroupsandTagEditorReadOnlyAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:39 UTC
- 편집된 시간: 2023년 8월 10일, 13:42 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ResourceGroupsServiceRolePolicy

`ResourceGroupsServiceRolePolicy`는 AWS 관리형 정책으로, AWS Resource Groups가 리소스를 소유한 AWS 서비스를 쿼리하여 그룹을 최신 상태로 유지할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2023년 1월 5일, 16:57 UTC
- 편집된 시간: 2023년 1월 5일, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy는 AWS 관리형 정책으로, OpenShift Amazon EBS Container Storage Interface(CSI) Driver Operator가 Red Hat OpenShift Service on AWS(ROSA) 클러스터에 Amazon EBS CSI 드라이버를 설치하고 유지 관리할 수 있도록 허용합니다. Amazon EBS CSI 드라이버를 사용하면 ROSA 클러스터가 영구 볼륨에 대한 Amazon EBS 볼륨의 수명 주기를 관리할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAAmazonEBSCSIDriverOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:36 UTC
- 편집된 시간: 2023년 4월 20일, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy는 AWS 관리형 정책으로, OpenShift Cloud Network Config Controller Operator가 Red Hat OpenShift Service on AWS(ROSA) 클러스터 네트워킹 오버레이에서 사용할 네트워킹 리소스를 프로비저닝하고 관리할 수 있도록 허용합니다. OpenShift Cloud Network Operator는 네트워크 플러그인을 대신하여 CustomResourceDefinitions를 통해 AWS API와 인터페이스합니다. 운영자는 이러한 정책 권한을 사용하여 ROSA 클러스터의 일부인 Amazon EC2 인스턴스의 프라이빗 IP 주소를 관리합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSACloudNetworkConfigOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:34 UTC

- 편집된 시간: 2023년 4월 20일, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAControlPlaneOperatorPolicy

ROSAControlPlaneOperatorPolicy는 AWS 관리형 정책으로, Red Hat OpenShift Service on AWS(ROSA) 컨트롤 플레인이 ROSA 클러스터 Amazon EC2 및 Amazon Route 53 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAControlPlaneOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 24일, 23:02 UTC
- 편집된 시간: 2023년 6월 30일, 21:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAImageRegistryOperatorPolicy

`ROSAImageRegistryOperatorPolicy`ROSA 스토리지 요구 사항을 충족하기 위해 Red Hat OpenShift Service on AWS (ROSA) 클러스터 내 OpenShift 이미지 레지스트리에서 사용할 Amazon S3 버킷과 객체를 이미지 레지스트리 운영자가 프로비저닝하고 관리하는 관리형 정책입니다. AWS OpenShift 이미지 레지스트리 운영자는 Red Hat 클러스터의 내부 레지스트리를 설치하고 유지 관리합니다. OpenShift

이 정책 사용

사용자, 그룹 및 역할에 `ROSAImageRegistryOperatorPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:13 UTC
- 편집 시간: 2023년 12월 12일 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
```

```
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAIngressOperatorPolicy

`ROSAIngressOperatorPolicy`는 AWS 관리형 정책으로, OpenShift Ingress Operator가 Red Hat OpenShift Service on AWS(ROSA) 클러스터에 대한 로드 밸런서 및 도메인 이름 시스템(DNS) 구성

을 프로비저닝하고 관리할 수 있도록 허용합니다. 이 정책은 운영자가 호스팅 영역을 검색하기 위해 Route 53 리소스를 필터링하는 태그 값에 대한 읽기 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAIngressOperatorPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:37 UTC
- 편집된 시간: 2023년 4월 20일, 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAInstallerPolicy

`ROSAInstallerPolicy`ROSA AWS (Red Hat OpenShift Service on) 설치 프로그램이 ROSA 클러스터 설치를 지원하는 AWS 리소스를 관리할 수 있도록 하는 AWS관리형 정책입니다. 여기에는 ROSA 워커 노드에 대한 인스턴스 프로파일 관리가 포함됩니다.

이 정책 사용

사용자, 그룹 및 역할에 `ROSAInstallerPolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 6일, 21:00 UTC
- 편집 시간: 2024년 1월 26일 21:04 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAKMSProviderPolicy

ROSAKMSProviderPolicy는 AWS 관리형 정책으로, 내장된 ROSA AWS 암호화 공급자가 AWS Key Management Service(KMS) 키를 관리하여 고객이 제공한 AWS KMS 키를 사용하여 etcd 데이터 암호화를 지원할 수 있도록 허용합니다. 이 정책은 KMS 키를 사용한 데이터 암호화 및 암호 해독을 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAKMSProviderPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:10 UTC
- 편집된 시간: 2023년 4월 27일, 20:10 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAKubeControllerPolicy

ROSAKubeControllerPolicy는 AWS 관리형 정책으로, ROSA Kubernetes 컨트롤러가 ROSA 클러스터에 대한 Amazon EC2, Elastic Load Balancing (ELB) 및 AWS Key Management Service(KMS) 리소스를 관리할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAKubeControllerPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 27일, 20:09 UTC
- 편집된 시간: 2023년 10월 16일, 18:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

정책 버전

정책 버전: v3(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAManageSubscription

`ROSAManageSubscription`는 AWS 관리형 정책으로, 이 정책은 Red Hat OpenShift Service on AWS(ROSA) 구독을 관리하는 데 필요한 권한을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ROSAManageSubscription`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2022년 4월 11일, 20:58 UTC
- 편집된 시간: 2023년 8월 4일, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSANodePoolManagementPolicy

`ROSANodePoolManagementPolicy`는 AWS 관리형 정책으로, Red Hat OpenShift Service on AWS(ROSA)가 보안 그룹을 구성하고 인스턴스 및 볼륨에 태그를 지정할 수 있는 권한을 포함하여 클러스터 EC2 인스턴스를 워커 노드로 관리할 수 있도록 허용합니다. 또한 이 정책은AWS Key Management Service(KMS) 키로 제공되는 디스크 암호화와 함께 EC2 인스턴스를 사용할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSANodePoolManagementPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 8일, 20:48 UTC
- 편집된 시간: 2023년 6월 8일, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSASRESupportPolicy

ROSASRESupportPolicyROSA 클러스터 노드 상태를 변경하는 기능을 포함하여 ROSA (ROSA) 클러스터에서 ROSA (Red Hat OpenShift Service) 와 관련된 AWS 리소스를 초기에 관찰, 진단 및 지원하는 데 필요한 권한을 ROSA 사이트 신뢰성 엔지니어링 AWS (SRE) 에 제공하는 AWS관리형 정책입니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSASRESupportPolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 6월 1일, 14:36 UTC
- 편집 시간: 2024년 1월 22일 22:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ROSAWorkerInstancePolicy

ROSAWorkerInstancePolicy는 AWS 관리형 정책으로, 컴퓨팅 노드 수명 주기 관리를 위해 계정의 Red Hat OpenShift Service on AWS(ROSA) 워커 노드에서 Amazon EC2 인스턴스 및 AWS 리전에 대한 읽기 전용 액세스와 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 ROSAWorkerInstancePolicy를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2023년 4월 20일, 22:35 UTC
- 편집된 시간: 2023년 4월 20일, 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Route53RecoveryReadinessServiceRolePolicy

`Route53RecoveryReadinessServiceRolePolicy`는 AWS 관리형 정책으로, Route 53 복구 준비를 위한 서비스 연결 역할 정책입니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2021년 7월 15일, 16:06 UTC
- 편집된 시간: 2023년 2월 14일, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

Route53ResolverServiceRolePolicy

`Route53ResolverServiceRolePolicy`는 AWS 관리형 정책으로, Route53 Resolver에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 8월 12일, 17:47 UTC
- 편집된 시간: 2020년 8월 12일, 17:47 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

S3StorageLensServiceRolePolicy

S3StorageLensServiceRolePolicy는 AWS 관리형 정책으로, S3 Storage Lens에서 사용하거나 관리하는 AWS 서비스 및 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2020년 11월 18일, 18:15 UTC
- 편집된 시간: 2020년 11월 18일, 18:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

SecretsManagerReadWrite

`SecretsManagerReadWrite`는 다음을 통해 AWS Secrets Manager에 대한 읽기/쓰기 액세스를 제공하는 AWS 관리형 정책입니다. AWS Management Console 참고: 여기에는 IAM 작업이 제외되므로 순환 구성이 필요한 경우 IAM과 함께 사용하십시오FullAccess .

이 정책 사용

사용자, 그룹 및 역할에 `SecretsManagerReadWrite`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 관리형 정책 AWS
- 생성 시간: 2018년 4월 4일, 18:05 UTC
- 편집 시간: 2024년 2월 22일 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

정책 버전

정책 버전: v5(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*/*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트를 생성합니다.
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

SecurityAudit

SecurityAudit는 AWS 관리형 정책으로, 보안 감사 템플릿이 보안 구성 메타데이터를 읽을 수 있는 액세스를 부여합니다. AWS 계정의 구성을 감사하는 소프트웨어에 유용합니다.

이 정책 사용

사용자, 그룹 및 역할에 SecurityAudit를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집 시간: 2023년 12월 14일 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

정책 버전

정책 버전: v41(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "BaseSecurityAuditStatement",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
```

```
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeRegionSettings",
```

```
        "backup:GetBackupVaultAccessPolicy",
        "backup:ListBackupVaults",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListTagsForResource",
        "cloudwatch:ListDashboards",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:ListProjects",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
```

```
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListInstances",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
```

```
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
```

```
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListUpdates",
        "elastic-inference:DescribeAccelerators",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
```

```
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfigurations",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
```

```
        "guardduty:List*",
        "health:DescribeAffectedEntities",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEvents",
        "health:DescribeEventTypes",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
```

```
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
```

```
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "machinelearning:DescribeMLModels",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
```

```
        "organizations:Describe*",
        "organizations:List*",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
```

```
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccountSendingEnabled",
```

```
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionsPolicies",
        "sso:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
```

```
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
```

```
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLforResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
```

```
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

SecurityLakeServiceLinkedRole

`SecurityLakeServiceLinkedRole`는 AWS 관리형 정책으로, 이 정책은 사용자를 대신하여 Amazon Security Lake 서비스를 운영할 수 있는 권한을 부여합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2022년 11월 29일, 14:03 UTC
- 편집 시간: 2024년 2월 29일 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 정책의 기본 버전을 AWS 확인하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환하세요.

ServerMigration_ServiceRole

`ServerMigration_ServiceRole`은 AWS 관리형 정책으로, AWS Server Migration Service가 VM을 EC2로 마이그레이션할 수 있도록 허용하는 권한으로, Server Migration Service가 마이그레이션된 리소스를 고객의 EC2 계정에 배치할 수 있도록 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ServerMigration_ServiceRole`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 8월 11일, 20:41 UTC
- 편집된 시간: 2020년 10월 15일, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성

- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServerMigrationConnector

`ServerMigrationConnector`는 AWS 관리형 정책으로, AWS Server Migration Connector가 VM을 EC2로 마이그레이션할 수 있도록 허용하는 권한입니다. AWS는 Server Migration Service와의 통신, 'sms-b-' 및 'import-to-ec2-'로 시작하는 S3 버킷뿐만 아니라 AWS Server Migration Connector 업그레이드, AWS에 AWS Server Migration Connector 등록 및 AWS에 지표 업로드에 사용되는 버킷에 대한 읽기/쓰기 액세스를 허용합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ServerMigrationConnector`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2016년 10월 24일, 21:45 UTC
- 편집된 시간: 2016년 10월 24일, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServerMigrationServiceConsoleFullAccess

`ServerMigrationServiceConsoleFullAccess`는 AWS 관리형 정책으로, Server Migration Service Console의 모든 기능을 사용하기 위해 필요한 권한입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ServerMigrationServiceConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2020년 5월 9일, 17:18 UTC
- 편집된 시간: 2020년 7월 20일, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole는 AWS 관리형 정책으로, AWS Server Migration Service가 마이그레이션된 서버 및 애플리케이션 실행을 위해 고객의 AWS 계정에 관련 AWS 리소스를 생성하고 업데이트할 수 있도록 허용하는 권한입니다.

이 정책 사용

사용자, 그룹 및 역할에 ServerMigrationServiceLaunchRole를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2018년 11월 26일, 19:53 UTC
- 편집된 시간: 2020년 10월 15일, 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServerMigrationServiceRoleForInstanceValidation

`ServerMigrationServiceRoleForInstanceValidation`는 AWS 관리형 정책으로, AWS SMS가 사용된 데이터 검증 스크립트를 실행하고 스크립트 성공/실패를 SMS로 다시 보낼 수 있도록 허용하는 권한입니다.

이 정책 사용

사용자, 그룹 및 역할에 `ServerMigrationServiceRoleForInstanceValidation`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2020년 7월 20일, 22:25 UTC
- 편집된 시간: 2020년 7월 20일, 22:25 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServiceQuotasFullAccess

ServiceQuotasFullAccess는 AWS 관리형 정책으로, Service Quotas에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 ServiceQuotasFullAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 24일, 15:44 UTC
- 편집된 시간: 2021년 2월 4일, 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

정책 버전

정책 버전: v4(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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"
        }
      }
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServiceQuotasReadOnlyAccess

`ServiceQuotasReadOnlyAccess`는 AWS 관리형 정책으로, Service Quotas에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ServiceQuotasReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 6월 24일, 15:31 UTC
- 편집된 시간: 2020년 12월 21일, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
```

```
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ServiceQuotasServiceRolePolicy

`ServiceQuotasServiceRolePolicy`는 AWS 관리형 정책으로, Service Quotas가 사용자를 대신하여 지원 사례를 생성할 수 있도록 허용합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 5월 22일, 20:44 UTC
- 편집된 시간: 2019년 6월 24일, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

SimpleWorkflowFullAccess

`SimpleWorkflowFullAccess`는 AWS 관리형 정책으로, Simple Workflow 구성 서비스에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `SimpleWorkflowFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2015년 2월 6일, 18:41 UTC
- 편집된 시간: 2015년 2월 6일, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

SupportUser

SupportUser는 AWS 관리형 정책으로, 이 정책은 AWS 계정의 문제를 해결하고 해결할 수 있는 권한을 부여합니다. 또한 이 정책을 통해 사용자는 AWS 지원팀에 문의하여 사례를 생성하고 관리할 수 있습니다.

이 정책 사용

사용자, 그룹 및 역할에 SupportUser를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:21 UTC
- 편집된 시간: 2023년 8월 25일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

정책 버전

정책 버전: v8(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

SystemAdministrator

`SystemAdministrator`는 AWS 관리형 정책으로, 애플리케이션 및 개발 작업에 필요한 리소스에 필요한 전체 액세스 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `SystemAdministrator`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:23 UTC
- 편집된 시간: 2020년 8월 24일, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

정책 버전

정책 버전: v6(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
```

```
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
```

```
            "ec2:DeleteSubnet",
            "ec2:DeleteTags",
            "ec2:DeleteVpc",
            "ec2:DeleteVpcEndpoints",
            "ec2:DeleteVpnConnection",
            "ec2:DeleteVpnConnectionRoute",
            "ec2:DeleteVpnGateway",
            "ec2:DeregisterImage",
            "ec2:Describe*",
            "ec2:DetachInternetGateway",
            "ec2:DetachNetworkInterface",
            "ec2:DetachVpnGateway",
            "ec2:DisableVgwRoutePropagation",
            "ec2:DisableVpcClassicLinkDnsSupport",
            "ec2:DisassociateAddress",
            "ec2:DisassociateRouteTable",
            "ec2:EnableVgwRoutePropagation",
            "ec2:EnableVolumeIO",
            "ec2:EnableVpcClassicLinkDnsSupport",
            "ec2:GetConsoleOutput",
            "ec2:GetHostReservationPurchasePreview",
            "ec2:GetLaunchTemplateData",
            "ec2:GetPasswordData",
            "ec2:Import*",
            "ec2:Modify*",
            "ec2:MonitorInstances",
            "ec2:MoveAddressToVpc",
            "ec2:Purchase*",
            "ec2:RegisterImage",
            "ec2:Release*",
            "ec2:Replace*",
            "ec2:ReportInstanceStatus",
            "ec2:Request*",
            "ec2:Reset*",
            "ec2:RestoreAddressToClassic",
            "ec2:RunScheduledInstances",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:UnmonitorInstances",
            "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
            "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
            "elasticloadbalancing:*",
            "events:*",
            "iam:GetAccount*",
            "iam:GetContextKeys*",
```

```
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
```

```
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
```

```
    }
  ],
  "Version" : "2012-10-17"
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

TranslateFullAccess

`TranslateFullAccess`는 AWS 관리형 정책으로, Amazon Translate에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `TranslateFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 27일, 23:36 UTC
- 편집된 시간: 2020년 1월 8일, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

TranslateReadOnly

`TranslateReadOnly`는 AWS 관리형 정책으로, Amazon Translate에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `TranslateReadOnly`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2017년 11월 29일, 18:22 UTC
- 편집된 시간: 2023년 5월 24일, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

정책 버전

정책 버전: v7(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

ViewOnlyAccess

`ViewOnlyAccess`는 AWS 관리형 정책으로, 이 정책은 모든 AWS 서비스에 걸쳐 리소스 및 기본 메타데이터를 볼 수 있는 권한을 부여합니다.

이 정책 사용

사용자, 그룹 및 역할에 `ViewOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: 직무 정책
- 생성 시간: 2016년 11월 10일, 17:20 UTC
- 편집된 시간: 2023년 3월 6일, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

정책 버전

정책 버전: v17(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "batch:ListJobs",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudhsm:ListAvailableZones",
        "cloudhsm:ListHapgs",
        "cloudhsm:ListHsms",
        "cloudhsm:ListLunaClients",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
```

```
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
```

```
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
```

```
        "elastictranscoder:List*",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kms:ListKeys",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBots",
        "lex:GetIntentVersions",
        "lex:GetIntents",
        "lex:GetSlotTypeVersions",
        "lex:GetSlotTypes",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
```

```
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:List*",
        "shield:List*",
        "sns:List*",
        "sqs:ListQueues",
```

```
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

VMImportExportRoleForAWSConnector

`VMImportExportRoleForAWSConnector`는 AWS 관리형 정책으로, AWS Connector를 사용하는 고객을 위한 VM Import/Export 서비스 역할에 대한 기본 정책입니다. VM Import/Export 서비스는 이 정책에 따라 AWS Connector 가상 어플라이언스의 가상 머신 마이그레이션 요청을 수행하는 역할을 맡습니다. (참고로 AWS Connector는 'AWSConnector' 관리형 정책을 사용하여 고객을 대신하여 VM Import/Export 서비스에 요청을 발행합니다.) AMI 및 EBS 스냅샷 생성, EBS 스냅샷 속성 수정, EC2 객체에 대해 'Describe*' 호출, 'import-to-ec2-'로 시작하는 S3 버킷에서 읽을 수 있는 기능을 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 VMImportExportRoleForAWSConnector를 연결할 수 있습니다.

정책 세부 정보

- 유형: 서비스 역할 정책
- 생성 시간: 2015년 9월 3일, 20:48 UTC
- 편집된 시간: 2015년 9월 3일, 20:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

VPCLatticeFullAccess

`VPCLatticeFullAccess`는 AWS 관리형 정책으로, Amazon VPC Lattice에 대한 전체 액세스 권한 및 종속성 서비스에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `VPCLatticeFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:49 UTC
- 편집된 시간: 2023년 3월 30일, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

VPCLatticeReadOnlyAccess

`VPCLatticeReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 Amazon VPC Lattice에 대한 읽기 전용 액세스를 제공하고 종속성 서비스에 대한 제한된 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `VPCLatticeReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:47 UTC
- 편집된 시간: 2023년 3월 30일, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

VPCLatticeServicesInvokeAccess

`VPCLatticeServicesInvokeAccess`는 AWS 관리형 정책으로, Amazon VPC Lattice 서비스 호출에 대한 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 VPCLatticeServicesInvokeAccess를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2023년 3월 30일, 02:45 UTC
- 편집된 시간: 2023년 3월 30일, 02:45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WAFLoggingServiceRolePolicy

WAFLoggingServiceRolePolicy는 AWS 관리형 정책으로, 고객의 로그를 Firehose 스트림에 기록하기 위한 SLR을 생성합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 24일, 21:05 UTC
- 편집된 시간: 2018년 8월 24일, 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
```

```
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WAFRegionalLoggingServiceRolePolicy

`WAFRegionalLoggingServiceRolePolicy`는 AWS 관리형 정책으로, 고객의 로그를 Firehose 스트림에 기록하기 위한 SLR을 생성합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2018년 8월 24일, 18:40 UTC
- 편집된 시간: 2018년 8월 24일, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WAFV2LoggingServiceRolePolicy

`WAFV2LoggingServiceRolePolicy`는 AWS 관리형 정책으로, 이 정책은 AWS WAF가 Amazon Kinesis Data Firehose에 로그를 쓸 수 있도록 하는 서비스 연결 역할을 생성합니다.

이 정책 사용

이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 사용자, 그룹 또는 역할에 정책을 연결할 수 없습니다.

정책 세부 정보

- 유형: 서비스 연결 역할 정책
- 생성 시간: 2019년 11월 7일, 00:40 UTC
- 편집된 시간: 2020년 7월 23일, 17:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WellArchitectedConsoleFullAccess

`WellArchitectedConsoleFullAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Well-Architected Tool에 대한 전체 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `WellArchitectedConsoleFullAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 18:19 UTC
- 편집된 시간: 2018년 11월 29일, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WellArchitectedConsoleReadOnlyAccess

`WellArchitectedConsoleReadOnlyAccess`는 AWS 관리형 정책으로, AWS Management Console을 통해 AWS Well-Architected Tool에 대한 읽기 전용 액세스를 제공합니다.

이 정책 사용

사용자, 그룹 및 역할에 `WellArchitectedConsoleReadOnlyAccess`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2018년 11월 29일, 18:21 UTC
- 편집된 시간: 2023년 6월 29일, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

정책 버전

정책 버전: v2(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

WorkLinkServiceRolePolicy

`WorkLinkServiceRolePolicy`는 AWS 관리형 정책으로, Amazon WorkLink에서 사용하거나 관리하는 AWS 서비스 리소스에 대한 액세스를 활성화합니다.

이 정책 사용

사용자, 그룹 및 역할에 `WorkLinkServiceRolePolicy`를 연결할 수 있습니다.

정책 세부 정보

- 유형: AWS 관리형 정책
- 생성 시간: 2019년 1월 23일, 19:03 UTC
- 편집된 시간: 2019년 1월 23일, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

정책 버전

정책 버전: v1(기본값)

정책의 기본 버전은 정책에 대한 권한을 정의하는 버전입니다. 정책이 적용되는 사용자 또는 역할이 AWS 리소스에 대한 액세스를 요청하면 AWS는 정책의 기본 버전을 검사하여 요청을 허용할지 여부를 결정합니다.

JSON 정책 문서

```
{
  "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-*"
    }
  ]
}
```

자세히 알아보기

- IAM Identity Center에서 AWS 관리형 정책을 사용하여 권한 세트 생성
- IAM 자격 증명 권한 추가 및 제거
- IAM 정책의 버전 관리 이해
- AWS 관리형 정책을 시작하고 최소 권한으로 전환

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.