



参考指南

AWS 托管策略



AWS 托管策略: 参考指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

| | |
|---|----|
| 什么是 AWS 托管策略？ | 1 |
| 了解策略参考页面 | 1 |
| 已弃用的 AWS 托管策略 | 2 |
| AWS 托管策略 | 3 |
| AccessAnalyzerServiceRolePolicy | 43 |
| 使用此策略 | 43 |
| 策略详细信息 | 43 |
| 策略版本 | 43 |
| JSON 策略文档 | 44 |
| 了解更多信息 | 46 |
| AdministratorAccess | 46 |
| 使用此策略 | 46 |
| 策略详细信息 | 46 |
| 策略版本 | 46 |
| JSON 策略文档 | 47 |
| 了解更多信息 | 47 |
| AdministratorAccess-Amplify | 47 |
| 使用此策略 | 47 |
| 策略详细信息 | 47 |
| 策略版本 | 48 |
| JSON 策略文档 | 48 |
| 了解更多信息 | 58 |
| AdministratorAccess-AWSElasticBeanstalk | 58 |
| 使用此策略 | 58 |
| 策略详细信息 | 58 |
| 策略版本 | 59 |
| JSON 策略文档 | 59 |
| 了解更多信息 | 67 |
| AlexaForBusinessDeviceSetup | 67 |
| 使用此策略 | 67 |
| 策略详细信息 | 67 |
| 策略版本 | 68 |
| JSON 策略文档 | 68 |
| 了解更多信息 | 68 |

| | |
|---|----|
| AlexaForBusinessFullAccess | 69 |
| 使用此策略 | 69 |
| 策略详细信息 | 69 |
| 策略版本 | 69 |
| JSON 策略文档 | 69 |
| 了解更多信息 | 71 |
| AlexaForBusinessGatewayExecution | 71 |
| 使用此策略 | 71 |
| 策略详细信息 | 71 |
| 策略版本 | 71 |
| JSON 策略文档 | 71 |
| 了解更多信息 | 72 |
| AlexaForBusinessLifesizeDelegatedAccessPolicy | 73 |
| 使用此策略 | 73 |
| 策略详细信息 | 73 |
| 策略版本 | 73 |
| JSON 策略文档 | 73 |
| 了解更多信息 | 75 |
| AlexaForBusinessNetworkProfileServicePolicy | 76 |
| 使用此策略 | 76 |
| 策略详细信息 | 76 |
| 策略版本 | 76 |
| JSON 策略文档 | 76 |
| 了解更多信息 | 77 |
| AlexaForBusinessPolyDelegatedAccessPolicy | 77 |
| 使用此策略 | 77 |
| 策略详细信息 | 77 |
| 策略版本 | 78 |
| JSON 策略文档 | 78 |
| 了解更多信息 | 79 |
| AlexaForBusinessReadOnlyAccess | 80 |
| 使用此策略 | 80 |
| 策略详细信息 | 80 |
| 策略版本 | 80 |
| JSON 策略文档 | 80 |
| 了解更多信息 | 81 |

| | |
|--|----|
| AmazonAPIGatewayAdministrator | 81 |
| 使用此策略 | 81 |
| 策略详细信息 | 81 |
| 策略版本 | 81 |
| JSON 策略文档 | 81 |
| 了解更多信息 | 82 |
| AmazonAPIGatewayInvokeFullAccess | 82 |
| 使用此策略 | 82 |
| 策略详细信息 | 82 |
| 策略版本 | 82 |
| JSON 策略文档 | 83 |
| 了解更多信息 | 83 |
| AmazonAPIGatewayPushToCloudWatchLogs | 83 |
| 使用此策略 | 83 |
| 策略详细信息 | 83 |
| 策略版本 | 84 |
| JSON 策略文档 | 84 |
| 了解更多信息 | 84 |
| AmazonAppFlowFullAccess | 85 |
| 使用此策略 | 85 |
| 策略详细信息 | 85 |
| 策略版本 | 85 |
| JSON 策略文档 | 85 |
| 了解更多信息 | 88 |
| AmazonAppFlowReadOnlyAccess | 88 |
| 使用此策略 | 88 |
| 策略详细信息 | 88 |
| 策略版本 | 89 |
| JSON 策略文档 | 89 |
| 了解更多信息 | 89 |
| AmazonAppStreamFullAccess | 90 |
| 使用此策略 | 90 |
| 策略详细信息 | 90 |
| 策略版本 | 90 |
| JSON 策略文档 | 90 |
| 了解更多信息 | 92 |

| | |
|--|-----|
| AmazonAppStreamPCAAccess | 92 |
| 使用此策略 | 92 |
| 策略详细信息 | 92 |
| 策略版本 | 93 |
| JSON 策略文档 | 93 |
| 了解更多信息 | 93 |
| AmazonAppStreamReadOnlyAccess | 94 |
| 使用此策略 | 94 |
| 策略详细信息 | 94 |
| 策略版本 | 94 |
| JSON 策略文档 | 94 |
| 了解更多信息 | 95 |
| AmazonAppStreamServiceAccess | 95 |
| 使用此策略 | 95 |
| 策略详细信息 | 95 |
| 策略版本 | 95 |
| JSON 策略文档 | 95 |
| 了解更多信息 | 97 |
| AmazonAthenaFullAccess | 97 |
| 使用此策略 | 97 |
| 策略详细信息 | 97 |
| 策略版本 | 97 |
| JSON 策略文档 | 97 |
| 了解更多信息 | 101 |
| AmazonAugmentedAIFullAccess | 101 |
| 使用此策略 | 101 |
| 策略详细信息 | 101 |
| 策略版本 | 101 |
| JSON 策略文档 | 102 |
| 了解更多信息 | 103 |
| AmazonAugmentedAIHumanLoopFullAccess | 103 |
| 使用此策略 | 103 |
| 策略详细信息 | 103 |
| 策略版本 | 103 |
| JSON 策略文档 | 103 |
| 了解更多信息 | 104 |

| | |
|---|-----|
| AmazonAugmentedAllIntegratedAPIAccess | 104 |
| 使用此策略 | 104 |
| 策略详细信息 | 104 |
| 策略版本 | 104 |
| JSON 策略文档 | 105 |
| 了解更多信息 | 106 |
| AmazonBedrockFullAccess | 106 |
| 使用此策略 | 106 |
| 策略详细信息 | 106 |
| 策略版本 | 107 |
| JSON 策略文档 | 107 |
| 了解更多信息 | 108 |
| AmazonBedrockReadOnly | 108 |
| 使用此策略 | 108 |
| 策略详细信息 | 108 |
| 策略版本 | 109 |
| JSON 策略文档 | 109 |
| 了解更多信息 | 109 |
| AmazonBraketFullAccess | 110 |
| 使用此策略 | 110 |
| 策略详细信息 | 110 |
| 策略版本 | 110 |
| JSON 策略文档 | 110 |
| 了解更多信息 | 114 |
| AmazonBraketJobsExecutionPolicy | 114 |
| 使用此策略 | 115 |
| 策略详细信息 | 115 |
| 策略版本 | 115 |
| JSON 策略文档 | 115 |
| 了解更多信息 | 118 |
| AmazonBraketServiceRolePolicy | 118 |
| 使用此策略 | 118 |
| 策略详细信息 | 118 |
| 策略版本 | 118 |
| JSON 策略文档 | 118 |
| 了解更多信息 | 119 |

| | |
|---|-----|
| AmazonChimeFullAccess | 119 |
| 使用此策略 | 119 |
| 策略详细信息 | 119 |
| 策略版本 | 120 |
| JSON 策略文档 | 120 |
| 了解更多信息 | 122 |
| AmazonChimeReadOnly | 122 |
| 使用此策略 | 122 |
| 策略详细信息 | 122 |
| 策略版本 | 123 |
| JSON 策略文档 | 123 |
| 了解更多信息 | 123 |
| AmazonChimeSDK | 123 |
| 使用此策略 | 123 |
| 策略详细信息 | 124 |
| 策略版本 | 124 |
| JSON 策略文档 | 124 |
| 了解更多信息 | 125 |
| AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy | 125 |
| 使用此策略 | 125 |
| 策略详细信息 | 125 |
| 策略版本 | 126 |
| JSON 策略文档 | 126 |
| 了解更多信息 | 127 |
| AmazonChimeSDKMessagingServiceRolePolicy | 127 |
| 使用此策略 | 127 |
| 策略详细信息 | 127 |
| 策略版本 | 128 |
| JSON 策略文档 | 128 |
| 了解更多信息 | 129 |
| AmazonChimeServiceRolePolicy | 129 |
| 使用此策略 | 129 |
| 策略详细信息 | 129 |
| 策略版本 | 129 |
| JSON 策略文档 | 129 |
| 了解更多信息 | 130 |

| | |
|--|-----|
| AmazonChimeTranscriptionServiceLinkedRolePolicy | 130 |
| 使用此策略 | 130 |
| 策略详细信息 | 130 |
| 策略版本 | 131 |
| JSON 策略文档 | 131 |
| 了解更多信息 | 131 |
| AmazonChimeUserManagement | 131 |
| 使用此策略 | 131 |
| 策略详细信息 | 132 |
| 策略版本 | 132 |
| JSON 策略文档 | 132 |
| 了解更多信息 | 133 |
| AmazonChimeVoiceConnectorServiceLinkedRolePolicy | 133 |
| 使用此策略 | 133 |
| 策略详细信息 | 134 |
| 策略版本 | 134 |
| JSON 策略文档 | 134 |
| 了解更多信息 | 136 |
| AmazonCloudDirectoryFullAccess | 136 |
| 使用此策略 | 136 |
| 策略详细信息 | 136 |
| 策略版本 | 136 |
| JSON 策略文档 | 136 |
| 了解更多信息 | 137 |
| AmazonCloudDirectoryReadOnlyAccess | 137 |
| 使用此策略 | 137 |
| 策略详细信息 | 137 |
| 策略版本 | 138 |
| JSON 策略文档 | 138 |
| 了解更多信息 | 138 |
| AmazonCloudWatchEvidentlyFullAccess | 138 |
| 使用此策略 | 139 |
| 策略详细信息 | 139 |
| 策略版本 | 139 |
| JSON 策略文档 | 139 |
| 了解更多信息 | 141 |

| | |
|--|-----|
| AmazonCloudWatchEvidentlyReadOnlyAccess | 142 |
| 使用此策略 | 142 |
| 策略详细信息 | 142 |
| 策略版本 | 142 |
| JSON 策略文档 | 142 |
| 了解更多信息 | 143 |
| AmazonCloudWatchEvidentlyServiceRolePolicy | 143 |
| 使用此策略 | 143 |
| 策略详细信息 | 143 |
| 策略版本 | 144 |
| JSON 策略文档 | 144 |
| 了解更多信息 | 145 |
| AmazonCloudWatchRUMFullAccess | 145 |
| 使用此策略 | 145 |
| 策略详细信息 | 146 |
| 策略版本 | 146 |
| JSON 策略文档 | 146 |
| 了解更多信息 | 148 |
| AmazonCloudWatchRUMReadOnlyAccess | 149 |
| 使用此策略 | 149 |
| 策略详细信息 | 149 |
| 策略版本 | 149 |
| JSON 策略文档 | 149 |
| 了解更多信息 | 150 |
| AmazonCloudWatchRUMServiceRolePolicy | 150 |
| 使用此策略 | 150 |
| 策略详细信息 | 150 |
| 策略版本 | 150 |
| JSON 策略文档 | 150 |
| 了解更多信息 | 151 |
| AmazonCodeCatalystFullAccess | 151 |
| 使用此策略 | 151 |
| 策略详细信息 | 152 |
| 策略版本 | 152 |
| JSON 策略文档 | 152 |
| 了解更多信息 | 153 |

| | |
|--|-----|
| AmazonCodeCatalystReadOnlyAccess | 153 |
| 使用此策略 | 153 |
| 策略详细信息 | 153 |
| 策略版本 | 153 |
| JSON 策略文档 | 154 |
| 了解更多信息 | 154 |
| AmazonCodeCatalystSupportAccess | 154 |
| 使用此策略 | 154 |
| 策略详细信息 | 154 |
| 策略版本 | 155 |
| JSON 策略文档 | 155 |
| 了解更多信息 | 155 |
| AmazonCodeGuruProfilerAgentAccess | 156 |
| 使用此策略 | 156 |
| 策略详细信息 | 156 |
| 策略版本 | 156 |
| JSON 策略文档 | 156 |
| 了解更多信息 | 157 |
| AmazonCodeGuruProfilerFullAccess | 157 |
| 使用此策略 | 157 |
| 策略详细信息 | 157 |
| 策略版本 | 157 |
| JSON 策略文档 | 157 |
| 了解更多信息 | 158 |
| AmazonCodeGuruProfilerReadOnlyAccess | 158 |
| 使用此策略 | 159 |
| 策略详细信息 | 159 |
| 策略版本 | 159 |
| JSON 策略文档 | 159 |
| 了解更多信息 | 160 |
| AmazonCodeGuruReviewerFullAccess | 160 |
| 使用此策略 | 160 |
| 策略详细信息 | 160 |
| 策略版本 | 160 |
| JSON 策略文档 | 160 |
| 了解更多信息 | 163 |

| | |
|---|-----|
| AmazonCodeGuruReviewerReadOnlyAccess | 163 |
| 使用此策略 | 163 |
| 策略详细信息 | 163 |
| 策略版本 | 164 |
| JSON 策略文档 | 164 |
| 了解更多信息 | 164 |
| AmazonCodeGuruReviewerServiceRolePolicy | 164 |
| 使用此策略 | 165 |
| 策略详细信息 | 165 |
| 策略版本 | 165 |
| JSON 策略文档 | 165 |
| 了解更多信息 | 167 |
| AmazonCodeGuruSecurityFullAccess | 167 |
| 使用此策略 | 167 |
| 策略详细信息 | 167 |
| 策略版本 | 168 |
| JSON 策略文档 | 168 |
| 了解更多信息 | 168 |
| AmazonCodeGuruSecurityScanAccess | 168 |
| 使用此策略 | 168 |
| 策略详细信息 | 169 |
| 策略版本 | 169 |
| JSON 策略文档 | 169 |
| 了解更多信息 | 169 |
| AmazonCognitoDeveloperAuthenticatedIdentities | 170 |
| 使用此策略 | 170 |
| 策略详细信息 | 170 |
| 策略版本 | 170 |
| JSON 策略文档 | 170 |
| 了解更多信息 | 171 |
| AmazonCognitoIdpEmailServiceRolePolicy | 171 |
| 使用此策略 | 171 |
| 策略详细信息 | 171 |
| 策略版本 | 171 |
| JSON 策略文档 | 172 |
| 了解更多信息 | 172 |

| | |
|--|-----|
| AmazonCognitoDpServiceRolePolicy | 172 |
| 使用此策略 | 172 |
| 策略详细信息 | 172 |
| 策略版本 | 173 |
| JSON 策略文档 | 173 |
| 了解更多信息 | 173 |
| AmazonCognitoPowerUser | 173 |
| 使用此策略 | 174 |
| 策略详细信息 | 174 |
| 策略版本 | 174 |
| JSON 策略文档 | 174 |
| 了解更多信息 | 175 |
| AmazonCognitoReadOnly | 176 |
| 使用此策略 | 176 |
| 策略详细信息 | 176 |
| 策略版本 | 176 |
| JSON 策略文档 | 176 |
| 了解更多信息 | 177 |
| AmazonCognitoUnAuthedIdentitiesSessionPolicy | 177 |
| 使用此策略 | 177 |
| 策略详细信息 | 177 |
| 策略版本 | 178 |
| JSON 策略文档 | 178 |
| 了解更多信息 | 178 |
| AmazonCognitoUnauthenticatedIdentities | 179 |
| 使用此策略 | 179 |
| 策略详细信息 | 179 |
| 策略版本 | 179 |
| JSON 策略文档 | 179 |
| 了解更多信息 | 180 |
| AmazonConnect_FullAccess | 180 |
| 使用此策略 | 180 |
| 策略详细信息 | 180 |
| 策略版本 | 180 |
| JSON 策略文档 | 180 |
| 了解更多信息 | 183 |

| | |
|---|-----|
| AmazonConnectCampaignsServiceLinkedRolePolicy | 183 |
| 使用此策略 | 183 |
| 策略详细信息 | 183 |
| 策略版本 | 184 |
| JSON 策略文档 | 184 |
| 了解更多信息 | 184 |
| AmazonConnectReadOnlyAccess | 185 |
| 使用此策略 | 185 |
| 策略详细信息 | 185 |
| 策略版本 | 185 |
| JSON 策略文档 | 185 |
| 了解更多信息 | 186 |
| AmazonConnectServiceLinkedRolePolicy | 186 |
| 使用此策略 | 186 |
| 策略详细信息 | 186 |
| 策略版本 | 186 |
| JSON 策略文档 | 187 |
| 了解更多信息 | 191 |
| AmazonConnectSynchronizationServiceRolePolicy | 191 |
| 使用此策略 | 191 |
| 策略详细信息 | 192 |
| 策略版本 | 192 |
| JSON 策略文档 | 192 |
| 了解更多信息 | 194 |
| AmazonConnectVoiceIDFullAccess | 194 |
| 使用此策略 | 194 |
| 策略详细信息 | 194 |
| 策略版本 | 195 |
| JSON 策略文档 | 195 |
| 了解更多信息 | 195 |
| AmazonDataZoneDomainExecutionRolePolicy | 195 |
| 使用此策略 | 195 |
| 策略详细信息 | 196 |
| 策略版本 | 196 |
| JSON 策略文档 | 196 |
| 了解更多信息 | 199 |

| | |
|--|-----|
| AmazonDataZoneEnvironmentRolePermissionsBoundary | 199 |
| 使用此策略 | 199 |
| 策略详细信息 | 199 |
| 策略版本 | 199 |
| JSON 策略文档 | 200 |
| 了解更多信息 | 212 |
| AmazonDataZoneFullAccess | 213 |
| 使用此策略 | 213 |
| 策略详细信息 | 213 |
| 策略版本 | 213 |
| JSON 策略文档 | 213 |
| 了解更多信息 | 216 |
| AmazonDataZoneFullUserAccess | 217 |
| 使用此策略 | 217 |
| 策略详细信息 | 217 |
| 策略版本 | 217 |
| JSON 策略文档 | 217 |
| 了解更多信息 | 220 |
| AmazonDataZoneGlueManageAccessRolePolicy | 220 |
| 使用此策略 | 220 |
| 策略详细信息 | 220 |
| 策略版本 | 221 |
| JSON 策略文档 | 221 |
| 了解更多信息 | 224 |
| AmazonDataZonePortalFullAccessPolicy | 225 |
| 使用此策略 | 225 |
| 策略详细信息 | 225 |
| 策略版本 | 225 |
| JSON 策略文档 | 225 |
| 了解更多信息 | 225 |
| AmazonDataZonePreviewConsoleFullAccess | 226 |
| 使用此策略 | 226 |
| 策略详细信息 | 226 |
| 策略版本 | 226 |
| JSON 策略文档 | 226 |
| 了解更多信息 | 228 |

| | |
|--|-----|
| AmazonDataZoneProjectDeploymentPermissionsBoundary | 228 |
| 使用此策略 | 229 |
| 策略详细信息 | 229 |
| 策略版本 | 229 |
| JSON 策略文档 | 229 |
| 了解更多信息 | 237 |
| AmazonDataZoneProjectRolePermissionsBoundary | 237 |
| 使用此策略 | 237 |
| 策略详细信息 | 237 |
| 策略版本 | 238 |
| JSON 策略文档 | 238 |
| 了解更多信息 | 245 |
| AmazonDataZoneRedshiftGlueProvisioningPolicy | 245 |
| 使用此策略 | 245 |
| 策略详细信息 | 245 |
| 策略版本 | 246 |
| JSON 策略文档 | 246 |
| 了解更多信息 | 253 |
| AmazonDataZoneRedshiftManageAccessRolePolicy | 254 |
| 使用此策略 | 254 |
| 策略详细信息 | 254 |
| 策略版本 | 254 |
| JSON 策略文档 | 254 |
| 了解更多信息 | 256 |
| AmazonDetectiveFullAccess | 257 |
| 使用此策略 | 257 |
| 策略详细信息 | 257 |
| 策略版本 | 257 |
| JSON 策略文档 | 257 |
| 了解更多信息 | 258 |
| AmazonDetectiveInvestigatorAccess | 258 |
| 使用此策略 | 259 |
| 策略详细信息 | 259 |
| 策略版本 | 259 |
| JSON 策略文档 | 259 |
| 了解更多信息 | 261 |

| | |
|--|-----|
| AmazonDetectiveMemberAccess | 261 |
| 使用此策略 | 261 |
| 策略详细信息 | 261 |
| 策略版本 | 261 |
| JSON 策略文档 | 261 |
| 了解更多信息 | 262 |
| AmazonDetectiveOrganizationsAccess | 262 |
| 使用此策略 | 262 |
| 策略详细信息 | 262 |
| 策略版本 | 263 |
| JSON 策略文档 | 263 |
| 了解更多信息 | 264 |
| AmazonDetectiveServiceLinkedRolePolicy | 265 |
| 使用此策略 | 265 |
| 策略详细信息 | 265 |
| 策略版本 | 265 |
| JSON 策略文档 | 265 |
| 了解更多信息 | 266 |
| AmazonDevOpsGuruConsoleFullAccess | 266 |
| 使用此策略 | 266 |
| 策略详细信息 | 266 |
| 策略版本 | 266 |
| JSON 策略文档 | 266 |
| 了解更多信息 | 269 |
| AmazonDevOpsGuruFullAccess | 269 |
| 使用此策略 | 269 |
| 策略详细信息 | 269 |
| 策略版本 | 269 |
| JSON 策略文档 | 270 |
| 了解更多信息 | 272 |
| AmazonDevOpsGuruOrganizationsAccess | 272 |
| 使用此策略 | 272 |
| 策略详细信息 | 272 |
| 策略版本 | 272 |
| JSON 策略文档 | 273 |
| 了解更多信息 | 274 |

| | |
|--|-----|
| AmazonDevOpsGuruReadOnlyAccess | 274 |
| 使用此策略 | 274 |
| 策略详细信息 | 274 |
| 策略版本 | 275 |
| JSON 策略文档 | 275 |
| 了解更多信息 | 277 |
| AmazonDevOpsGuruServiceRolePolicy | 277 |
| 使用此策略 | 277 |
| 策略详细信息 | 277 |
| 策略版本 | 277 |
| JSON 策略文档 | 277 |
| 了解更多信息 | 281 |
| AmazonDMSCloudWatchLogsRole | 282 |
| 使用此策略 | 282 |
| 策略详细信息 | 282 |
| 策略版本 | 282 |
| JSON 策略文档 | 282 |
| 了解更多信息 | 284 |
| AmazonDMSRedshiftS3Role | 284 |
| 使用此策略 | 284 |
| 策略详细信息 | 284 |
| 策略版本 | 284 |
| JSON 策略文档 | 284 |
| 了解更多信息 | 285 |
| AmazonDMSVPCManagementRole | 285 |
| 使用此策略 | 286 |
| 策略详细信息 | 286 |
| 策略版本 | 286 |
| JSON 策略文档 | 286 |
| 了解更多信息 | 287 |
| AmazonDocDB-ElasticServiceRolePolicy | 287 |
| 使用此策略 | 287 |
| 策略详细信息 | 287 |
| 策略版本 | 287 |
| JSON 策略文档 | 287 |
| 了解更多信息 | 288 |

| | |
|--|-----|
| AmazonDocDBConsoleFullAccess | 288 |
| 使用此策略 | 288 |
| 策略详细信息 | 288 |
| 策略版本 | 289 |
| JSON 策略文档 | 289 |
| 了解更多信息 | 293 |
| AmazonDocDBElasticFullAccess | 293 |
| 使用此策略 | 293 |
| 策略详细信息 | 293 |
| 策略版本 | 294 |
| JSON 策略文档 | 294 |
| 了解更多信息 | 297 |
| AmazonDocDBElasticReadOnlyAccess | 297 |
| 使用此策略 | 297 |
| 策略详细信息 | 297 |
| 策略版本 | 297 |
| JSON 策略文档 | 297 |
| 了解更多信息 | 298 |
| AmazonDocDBFullAccess | 298 |
| 使用此策略 | 298 |
| 策略详细信息 | 299 |
| 策略版本 | 299 |
| JSON 策略文档 | 299 |
| 了解更多信息 | 302 |
| AmazonDocDBReadOnlyAccess | 302 |
| 使用此策略 | 302 |
| 策略详细信息 | 302 |
| 策略版本 | 302 |
| JSON 策略文档 | 302 |
| 了解更多信息 | 304 |
| AmazonDRSVPCManagement | 304 |
| 使用此策略 | 305 |
| 策略详细信息 | 305 |
| 策略版本 | 305 |
| JSON 策略文档 | 305 |
| 了解更多信息 | 306 |

| | |
|--|-----|
| AmazonDynamoDBFullAccess | 306 |
| 使用此策略 | 306 |
| 策略详细信息 | 306 |
| 策略版本 | 306 |
| JSON 策略文档 | 307 |
| 了解更多信息 | 309 |
| AmazonDynamoDBFullAccesswithDataPipeline | 309 |
| 使用此策略 | 310 |
| 策略详细信息 | 310 |
| 策略版本 | 310 |
| JSON 策略文档 | 310 |
| 了解更多信息 | 312 |
| AmazonDynamoDBReadOnlyAccess | 312 |
| 使用此策略 | 312 |
| 策略详细信息 | 313 |
| 策略版本 | 313 |
| JSON 策略文档 | 313 |
| 了解更多信息 | 315 |
| AmazonEBSCSIDriverPolicy | 315 |
| 使用此策略 | 315 |
| 策略详细信息 | 315 |
| 策略版本 | 315 |
| JSON 策略文档 | 315 |
| 了解更多信息 | 319 |
| AmazonEC2ContainerRegistryFullAccess | 319 |
| 使用此策略 | 319 |
| 策略详细信息 | 319 |
| 策略版本 | 319 |
| JSON 策略文档 | 319 |
| 了解更多信息 | 320 |
| AmazonEC2ContainerRegistryPowerUser | 320 |
| 使用此策略 | 320 |
| 策略详细信息 | 321 |
| 策略版本 | 321 |
| JSON 策略文档 | 321 |
| 了解更多信息 | 322 |

| | |
|--|-----|
| AmazonEC2ContainerRegistryReadOnly | 322 |
| 使用此策略 | 322 |
| 策略详细信息 | 322 |
| 策略版本 | 322 |
| JSON 策略文档 | 322 |
| 了解更多信息 | 323 |
| AmazonEC2ContainerServiceAutoscaleRole | 323 |
| 使用此策略 | 323 |
| 策略详细信息 | 324 |
| 策略版本 | 324 |
| JSON 策略文档 | 324 |
| 了解更多信息 | 325 |
| AmazonEC2ContainerServiceEventsRole | 325 |
| 使用此策略 | 325 |
| 策略详细信息 | 325 |
| 策略版本 | 325 |
| JSON 策略文档 | 325 |
| 了解更多信息 | 326 |
| AmazonEC2ContainerServiceforEC2Role | 327 |
| 使用此策略 | 327 |
| 策略详细信息 | 327 |
| 策略版本 | 327 |
| JSON 策略文档 | 327 |
| 了解更多信息 | 328 |
| AmazonEC2ContainerServiceRole | 329 |
| 使用此策略 | 329 |
| 策略详细信息 | 329 |
| 策略版本 | 329 |
| JSON 策略文档 | 329 |
| 了解更多信息 | 330 |
| AmazonEC2FullAccess | 330 |
| 使用此策略 | 330 |
| 策略详细信息 | 330 |
| 策略版本 | 330 |
| JSON 策略文档 | 331 |
| 了解更多信息 | 332 |

| | |
|--|-----|
| AmazonEC2ReadOnlyAccess | 332 |
| 使用此策略 | 332 |
| 策略详细信息 | 332 |
| 策略版本 | 332 |
| JSON 策略文档 | 332 |
| 了解更多信息 | 333 |
| AmazonEC2RoleforAWSCodeDeploy | 333 |
| 使用此策略 | 334 |
| 策略详细信息 | 334 |
| 策略版本 | 334 |
| JSON 策略文档 | 334 |
| 了解更多信息 | 334 |
| AmazonEC2RoleforAWSCodeDeployLimited | 335 |
| 使用此策略 | 335 |
| 策略详细信息 | 335 |
| 策略版本 | 335 |
| JSON 策略文档 | 335 |
| 了解更多信息 | 336 |
| AmazonEC2RoleforDataPipelineRole | 336 |
| 使用此策略 | 336 |
| 策略详细信息 | 336 |
| 策略版本 | 337 |
| JSON 策略文档 | 337 |
| 了解更多信息 | 338 |
| AmazonEC2RoleforSSM | 338 |
| 使用此策略 | 338 |
| 策略详细信息 | 338 |
| 策略版本 | 338 |
| JSON 策略文档 | 338 |
| 了解更多信息 | 341 |
| AmazonEC2RolePolicyForLaunchWizard | 341 |
| 使用此策略 | 341 |
| 策略详细信息 | 341 |
| 策略版本 | 341 |
| JSON 策略文档 | 341 |
| 了解更多信息 | 345 |

| | |
|--|-----|
| AmazonEC2SpotFleetAutoscaleRole | 346 |
| 使用此策略 | 346 |
| 策略详细信息 | 346 |
| 策略版本 | 346 |
| JSON 策略文档 | 346 |
| 了解更多信息 | 347 |
| AmazonEC2SpotFleetTaggingRole | 347 |
| 使用此策略 | 347 |
| 策略详细信息 | 348 |
| 策略版本 | 348 |
| JSON 策略文档 | 348 |
| 了解更多信息 | 349 |
| AmazonECS_FullAccess | 350 |
| 使用此策略 | 350 |
| 策略详细信息 | 350 |
| 策略版本 | 350 |
| JSON 策略文档 | 350 |
| 了解更多信息 | 355 |
| AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity | 356 |
| 使用此策略 | 356 |
| 策略详细信息 | 356 |
| 策略版本 | 356 |
| JSON 策略文档 | 356 |
| 了解更多信息 | 359 |
| AmazonECSInfrastructureRolePolicyForVolumes | 359 |
| 使用此策略 | 359 |
| 策略详细信息 | 359 |
| 策略版本 | 359 |
| JSON 策略文档 | 359 |
| 了解更多信息 | 361 |
| AmazonECSServiceRolePolicy | 362 |
| 使用此策略 | 362 |
| 策略详细信息 | 362 |
| 策略版本 | 362 |
| JSON 策略文档 | 362 |
| 了解更多信息 | 367 |

| | |
|--|-----|
| AmazonECSTaskExecutionRolePolicy | 367 |
| 使用此策略 | 367 |
| 策略详细信息 | 367 |
| 策略版本 | 367 |
| JSON 策略文档 | 368 |
| 了解更多信息 | 368 |
| AmazonEFSCSIDriverPolicy | 368 |
| 使用此策略 | 368 |
| 策略详细信息 | 369 |
| 策略版本 | 369 |
| JSON 策略文档 | 369 |
| 了解更多信息 | 370 |
| AmazonEKS_CNI_Policy | 371 |
| 使用此策略 | 371 |
| 策略详细信息 | 371 |
| 策略版本 | 371 |
| JSON 策略文档 | 371 |
| 了解更多信息 | 372 |
| AmazonEKSClusterPolicy | 372 |
| 使用此策略 | 373 |
| 策略详细信息 | 373 |
| 策略版本 | 373 |
| JSON 策略文档 | 373 |
| 了解更多信息 | 375 |
| AmazonEKSClusterServiceRolePolicy | 375 |
| 使用此策略 | 375 |
| 策略详细信息 | 375 |
| 策略版本 | 376 |
| JSON 策略文档 | 376 |
| 了解更多信息 | 378 |
| AmazonEKSFargatePodExecutionRolePolicy | 378 |
| 使用此策略 | 378 |
| 策略详细信息 | 378 |
| 策略版本 | 378 |
| JSON 策略文档 | 378 |
| 了解更多信息 | 379 |

| | |
|--|-----|
| AmazonEKSFargateServiceRolePolicy | 379 |
| 使用此策略 | 379 |
| 策略详细信息 | 379 |
| 策略版本 | 379 |
| JSON 策略文档 | 380 |
| 了解更多信息 | 380 |
| AmazonEKSLocalOutpostClusterPolicy | 380 |
| 使用此策略 | 380 |
| 策略详细信息 | 381 |
| 策略版本 | 381 |
| JSON 策略文档 | 381 |
| 了解更多信息 | 383 |
| AmazonEKSLocalOutpostServiceRolePolicy | 383 |
| 使用此策略 | 383 |
| 策略详细信息 | 383 |
| 策略版本 | 383 |
| JSON 策略文档 | 384 |
| 了解更多信息 | 389 |
| AmazonEKSServicePolicy | 389 |
| 使用此策略 | 389 |
| 策略详细信息 | 389 |
| 策略版本 | 390 |
| JSON 策略文档 | 390 |
| 了解更多信息 | 391 |
| AmazonEKSServiceRolePolicy | 392 |
| 使用此策略 | 392 |
| 策略详细信息 | 392 |
| 策略版本 | 392 |
| JSON 策略文档 | 392 |
| 了解更多信息 | 395 |
| AmazonEKSVPCResourceController | 395 |
| 使用此策略 | 395 |
| 策略详细信息 | 395 |
| 策略版本 | 395 |
| JSON 策略文档 | 395 |
| 了解更多信息 | 396 |

| | |
|--|-----|
| AmazonEKSWorkerNodePolicy | 396 |
| 使用此策略 | 396 |
| 策略详细信息 | 396 |
| 策略版本 | 397 |
| JSON 策略文档 | 397 |
| 了解更多信息 | 397 |
| AmazonElastiCacheFullAccess | 398 |
| 使用此策略 | 398 |
| 策略详细信息 | 398 |
| 策略版本 | 398 |
| JSON 策略文档 | 398 |
| 了解更多信息 | 401 |
| AmazonElastiCacheReadOnlyAccess | 402 |
| 使用此策略 | 402 |
| 策略详细信息 | 402 |
| 策略版本 | 402 |
| JSON 策略文档 | 402 |
| 了解更多信息 | 403 |
| AmazonElasticContainerRegistryPublicFullAccess | 403 |
| 使用此策略 | 403 |
| 策略详细信息 | 403 |
| 策略版本 | 403 |
| JSON 策略文档 | 404 |
| 了解更多信息 | 404 |
| AmazonElasticContainerRegistryPublicPowerUser | 404 |
| 使用此策略 | 404 |
| 策略详细信息 | 404 |
| 策略版本 | 405 |
| JSON 策略文档 | 405 |
| 了解更多信息 | 405 |
| AmazonElasticContainerRegistryPublicReadOnly | 406 |
| 使用此策略 | 406 |
| 策略详细信息 | 406 |
| 策略版本 | 406 |
| JSON 策略文档 | 406 |
| 了解更多信息 | 407 |

| | |
|--|-----|
| AmazonElasticFileSystemClientFullAccess | 407 |
| 使用此策略 | 407 |
| 策略详细信息 | 407 |
| 策略版本 | 408 |
| JSON 策略文档 | 408 |
| 了解更多信息 | 408 |
| AmazonElasticFileSystemClientReadOnlyAccess | 408 |
| 使用此策略 | 409 |
| 策略详细信息 | 409 |
| 策略版本 | 409 |
| JSON 策略文档 | 409 |
| 了解更多信息 | 409 |
| AmazonElasticFileSystemClientReadWriteAccess | 410 |
| 使用此策略 | 410 |
| 策略详细信息 | 410 |
| 策略版本 | 410 |
| JSON 策略文档 | 410 |
| 了解更多信息 | 411 |
| AmazonElasticFileSystemFullAccess | 411 |
| 使用此策略 | 411 |
| 策略详细信息 | 411 |
| 策略版本 | 411 |
| JSON 策略文档 | 412 |
| 了解更多信息 | 413 |
| AmazonElasticFileSystemReadOnlyAccess | 414 |
| 使用此策略 | 414 |
| 策略详细信息 | 414 |
| 策略版本 | 414 |
| JSON 策略文档 | 414 |
| 了解更多信息 | 415 |
| AmazonElasticFileSystemServiceRolePolicy | 415 |
| 使用此策略 | 415 |
| 策略详细信息 | 415 |
| 策略版本 | 416 |
| JSON 策略文档 | 416 |
| 了解更多信息 | 418 |

| | |
|--|-----|
| AmazonElasticFileSystemsUtils | 418 |
| 使用此策略 | 418 |
| 策略详细信息 | 418 |
| 策略版本 | 418 |
| JSON 策略文档 | 419 |
| 了解更多信息 | 420 |
| AmazonElasticMapReduceEditorsRole | 421 |
| 使用此策略 | 421 |
| 策略详细信息 | 421 |
| 策略版本 | 421 |
| JSON 策略文档 | 421 |
| 了解更多信息 | 422 |
| AmazonElasticMapReduceforAutoScalingRole | 423 |
| 使用此策略 | 423 |
| 策略详细信息 | 423 |
| 策略版本 | 423 |
| JSON 策略文档 | 423 |
| 了解更多信息 | 424 |
| AmazonElasticMapReduceforEC2Role | 424 |
| 使用此策略 | 424 |
| 策略详细信息 | 424 |
| 策略版本 | 424 |
| JSON 策略文档 | 424 |
| 了解更多信息 | 426 |
| AmazonElasticMapReduceFullAccess | 426 |
| 使用此策略 | 426 |
| 策略详细信息 | 426 |
| 策略版本 | 427 |
| JSON 策略文档 | 427 |
| 了解更多信息 | 428 |
| AmazonElasticMapReducePlacementGroupPolicy | 429 |
| 使用此策略 | 429 |
| 策略详细信息 | 429 |
| 策略版本 | 429 |
| JSON 策略文档 | 429 |
| 了解更多信息 | 430 |

| | |
|--|-----|
| AmazonElasticMapReduceReadOnlyAccess | 430 |
| 使用此策略 | 430 |
| 策略详细信息 | 430 |
| 策略版本 | 430 |
| JSON 策略文档 | 431 |
| 了解更多信息 | 431 |
| AmazonElasticMapReduceRole | 431 |
| 使用此策略 | 431 |
| 策略详细信息 | 432 |
| 策略版本 | 432 |
| JSON 策略文档 | 432 |
| 了解更多信息 | 434 |
| AmazonElasticsearchServiceRolePolicy | 434 |
| 使用此策略 | 434 |
| 策略详细信息 | 434 |
| 策略版本 | 435 |
| JSON 策略文档 | 435 |
| 了解更多信息 | 438 |
| AmazonElasticTranscoder_FullAccess | 438 |
| 使用此策略 | 438 |
| 策略详细信息 | 438 |
| 策略版本 | 438 |
| JSON 策略文档 | 438 |
| 了解更多信息 | 439 |
| AmazonElasticTranscoder_JobsSubmitter | 439 |
| 使用此策略 | 440 |
| 策略详细信息 | 440 |
| 策略版本 | 440 |
| JSON 策略文档 | 440 |
| 了解更多信息 | 441 |
| AmazonElasticTranscoder_ReadOnlyAccess | 441 |
| 使用此策略 | 441 |
| 策略详细信息 | 441 |
| 策略版本 | 441 |
| JSON 策略文档 | 441 |
| 了解更多信息 | 442 |

| | |
|--|-----|
| AmazonElasticTranscoderRole | 442 |
| 使用此策略 | 442 |
| 策略详细信息 | 442 |
| 策略版本 | 443 |
| JSON 策略文档 | 443 |
| 了解更多信息 | 443 |
| AmazonEMRCleanupPolicy | 444 |
| 使用此策略 | 444 |
| 策略详细信息 | 444 |
| 策略版本 | 444 |
| JSON 策略文档 | 444 |
| 了解更多信息 | 445 |
| AmazonEMRContainersServiceRolePolicy | 445 |
| 使用此策略 | 445 |
| 策略详细信息 | 445 |
| 策略版本 | 446 |
| JSON 策略文档 | 446 |
| 了解更多信息 | 447 |
| AmazonEMRFullAccessPolicy_v2 | 447 |
| 使用此策略 | 447 |
| 策略详细信息 | 447 |
| 策略版本 | 447 |
| JSON 策略文档 | 448 |
| 了解更多信息 | 451 |
| AmazonEMRReadOnlyAccessPolicy_v2 | 451 |
| 使用此策略 | 451 |
| 策略详细信息 | 451 |
| 策略版本 | 452 |
| JSON 策略文档 | 452 |
| 了解更多信息 | 453 |
| AmazonEMRServerlessServiceRolePolicy | 453 |
| 使用此策略 | 453 |
| 策略详细信息 | 453 |
| 策略版本 | 453 |
| JSON 策略文档 | 454 |
| 了解更多信息 | 455 |

| | |
|---|-----|
| AmazonEMRServicePolicy_v2 | 455 |
| 使用此策略 | 455 |
| 策略详细信息 | 455 |
| 策略版本 | 455 |
| JSON 策略文档 | 455 |
| 了解更多信息 | 463 |
| AmazonESCognitoAccess | 463 |
| 使用此策略 | 463 |
| 策略详细信息 | 463 |
| 策略版本 | 463 |
| JSON 策略文档 | 464 |
| 了解更多信息 | 465 |
| AmazonESFullAccess | 465 |
| 使用此策略 | 465 |
| 策略详细信息 | 465 |
| 策略版本 | 465 |
| JSON 策略文档 | 465 |
| 了解更多信息 | 466 |
| AmazonESReadOnlyAccess | 466 |
| 使用此策略 | 466 |
| 策略详细信息 | 466 |
| 策略版本 | 466 |
| JSON 策略文档 | 467 |
| 了解更多信息 | 467 |
| AmazonEventBridgeApiDestinationsServiceRolePolicy | 467 |
| 使用此策略 | 467 |
| 策略详细信息 | 467 |
| 策略版本 | 468 |
| JSON 策略文档 | 468 |
| 了解更多信息 | 468 |
| AmazonEventBridgeFullAccess | 468 |
| 使用此策略 | 469 |
| 策略详细信息 | 469 |
| 策略版本 | 469 |
| JSON 策略文档 | 469 |
| 了解更多信息 | 471 |

| | |
|--|-----|
| AmazonEventBridgePipesFullAccess | 471 |
| 使用此策略 | 471 |
| 策略详细信息 | 472 |
| 策略版本 | 472 |
| JSON 策略文档 | 472 |
| 了解更多信息 | 473 |
| AmazonEventBridgePipesOperatorAccess | 473 |
| 使用此策略 | 473 |
| 策略详细信息 | 473 |
| 策略版本 | 473 |
| JSON 策略文档 | 473 |
| 了解更多信息 | 474 |
| AmazonEventBridgePipesReadOnlyAccess | 474 |
| 使用此策略 | 474 |
| 策略详细信息 | 474 |
| 策略版本 | 474 |
| JSON 策略文档 | 475 |
| 了解更多信息 | 475 |
| AmazonEventBridgeReadOnlyAccess | 475 |
| 使用此策略 | 475 |
| 策略详细信息 | 475 |
| 策略版本 | 476 |
| JSON 策略文档 | 476 |
| 了解更多信息 | 477 |
| AmazonEventBridgeSchedulerFullAccess | 477 |
| 使用此策略 | 478 |
| 策略详细信息 | 478 |
| 策略版本 | 478 |
| JSON 策略文档 | 478 |
| 了解更多信息 | 479 |
| AmazonEventBridgeSchedulerReadOnlyAccess | 479 |
| 使用此策略 | 479 |
| 策略详细信息 | 479 |
| 策略版本 | 479 |
| JSON 策略文档 | 479 |
| 了解更多信息 | 480 |

| | |
|---|-----|
| AmazonEventBridgeSchemasFullAccess | 480 |
| 使用此策略 | 480 |
| 策略详细信息 | 480 |
| 策略版本 | 481 |
| JSON 策略文档 | 481 |
| 了解更多信息 | 482 |
| AmazonEventBridgeSchemasReadOnlyAccess | 482 |
| 使用此策略 | 482 |
| 策略详细信息 | 482 |
| 策略版本 | 482 |
| JSON 策略文档 | 482 |
| 了解更多信息 | 483 |
| AmazonEventBridgeSchemasServiceRolePolicy | 483 |
| 使用此策略 | 483 |
| 策略详细信息 | 483 |
| 策略版本 | 484 |
| JSON 策略文档 | 484 |
| 了解更多信息 | 484 |
| AmazonFISServiceRolePolicy | 485 |
| 使用此策略 | 485 |
| 策略详细信息 | 485 |
| 策略版本 | 485 |
| JSON 策略文档 | 485 |
| 了解更多信息 | 487 |
| AmazonForecastFullAccess | 487 |
| 使用此策略 | 487 |
| 策略详细信息 | 487 |
| 策略版本 | 487 |
| JSON 策略文档 | 487 |
| 了解更多信息 | 488 |
| AmazonFraudDetectorFullAccessPolicy | 488 |
| 使用此策略 | 488 |
| 策略详细信息 | 489 |
| 策略版本 | 489 |
| JSON 策略文档 | 489 |
| 了解更多信息 | 490 |

| | |
|--------------------------------------|-----|
| AmazonFreeRTOSFullAccess | 490 |
| 使用此策略 | 490 |
| 策略详细信息 | 491 |
| 策略版本 | 491 |
| JSON 策略文档 | 491 |
| 了解更多信息 | 491 |
| AmazonFreeRTOSOTAUpdate | 492 |
| 使用此策略 | 492 |
| 策略详细信息 | 492 |
| 策略版本 | 492 |
| JSON 策略文档 | 492 |
| 了解更多信息 | 494 |
| AmazonFSxConsoleFullAccess | 494 |
| 使用此策略 | 494 |
| 策略详细信息 | 494 |
| 策略版本 | 494 |
| JSON 策略文档 | 494 |
| 了解更多信息 | 498 |
| AmazonFSxConsoleReadOnlyAccess | 498 |
| 使用此策略 | 498 |
| 策略详细信息 | 498 |
| 策略版本 | 498 |
| JSON 策略文档 | 499 |
| 了解更多信息 | 499 |
| AmazonFSxFullAccess | 499 |
| 使用此策略 | 500 |
| 策略详细信息 | 500 |
| 策略版本 | 500 |
| JSON 策略文档 | 500 |
| 了解更多信息 | 504 |
| AmazonFSxReadOnlyAccess | 504 |
| 使用此策略 | 504 |
| 策略详细信息 | 504 |
| 策略版本 | 505 |
| JSON 策略文档 | 505 |
| 了解更多信息 | 505 |

| | |
|-------------------------------------|-----|
| AmazonFSxServiceRolePolicy | 505 |
| 使用此策略 | 506 |
| 策略详细信息 | 506 |
| 策略版本 | 506 |
| JSON 策略文档 | 506 |
| 了解更多信息 | 509 |
| AmazonGlacierFullAccess | 509 |
| 使用此策略 | 509 |
| 策略详细信息 | 509 |
| 策略版本 | 509 |
| JSON 策略文档 | 510 |
| 了解更多信息 | 510 |
| AmazonGlacierReadOnlyAccess | 510 |
| 使用此策略 | 510 |
| 策略详细信息 | 510 |
| 策略版本 | 511 |
| JSON 策略文档 | 511 |
| 了解更多信息 | 511 |
| AmazonGrafanaAthenaAccess | 512 |
| 使用此策略 | 512 |
| 策略详细信息 | 512 |
| 策略版本 | 512 |
| JSON 策略文档 | 512 |
| 了解更多信息 | 514 |
| AmazonGrafanaCloudWatchAccess | 514 |
| 使用此策略 | 514 |
| 策略详细信息 | 514 |
| 策略版本 | 515 |
| JSON 策略文档 | 515 |
| 了解更多信息 | 516 |
| AmazonGrafanaRedshiftAccess | 516 |
| 使用此策略 | 516 |
| 策略详细信息 | 516 |
| 策略版本 | 517 |
| JSON 策略文档 | 517 |
| 了解更多信息 | 518 |

| | |
|---|-----|
| AmazonGrafanaServiceLinkedRolePolicy | 518 |
| 使用此策略 | 518 |
| 策略详细信息 | 518 |
| 策略版本 | 519 |
| JSON 策略文档 | 519 |
| 了解更多信息 | 520 |
| AmazonGuardDutyFullAccess | 520 |
| 使用此策略 | 520 |
| 策略详细信息 | 521 |
| 策略版本 | 521 |
| JSON 策略文档 | 521 |
| 了解更多信息 | 522 |
| AmazonGuardDutyMalwareProtectionServiceRolePolicy | 522 |
| 使用此策略 | 523 |
| 策略详细信息 | 523 |
| 策略版本 | 523 |
| JSON 策略文档 | 523 |
| 了解更多信息 | 527 |
| AmazonGuardDutyReadOnlyAccess | 528 |
| 使用此策略 | 528 |
| 策略详细信息 | 528 |
| 策略版本 | 528 |
| JSON 策略文档 | 528 |
| 了解更多信息 | 529 |
| AmazonGuardDutyServiceRolePolicy | 529 |
| 使用此策略 | 529 |
| 策略详细信息 | 529 |
| 策略版本 | 530 |
| JSON 策略文档 | 530 |
| 了解更多信息 | 534 |
| AmazonHealthLakeFullAccess | 535 |
| 使用此策略 | 535 |
| 策略详细信息 | 535 |
| 策略版本 | 535 |
| JSON 策略文档 | 535 |
| 了解更多信息 | 536 |

| | |
|--|-----|
| AmazonHealthLakeReadOnlyAccess | 536 |
| 使用此策略 | 536 |
| 策略详细信息 | 536 |
| 策略版本 | 536 |
| JSON 策略文档 | 537 |
| 了解更多信息 | 537 |
| AmazonHoneycodeFullAccess | 537 |
| 使用此策略 | 538 |
| 策略详细信息 | 538 |
| 策略版本 | 538 |
| JSON 策略文档 | 538 |
| 了解更多信息 | 538 |
| AmazonHoneycodeReadOnlyAccess | 539 |
| 使用此策略 | 539 |
| 策略详细信息 | 539 |
| 策略版本 | 539 |
| JSON 策略文档 | 539 |
| 了解更多信息 | 540 |
| AmazonHoneycodeServiceRolePolicy | 540 |
| 使用此策略 | 540 |
| 策略详细信息 | 540 |
| 策略版本 | 540 |
| JSON 策略文档 | 541 |
| 了解更多信息 | 541 |
| AmazonHoneycodeTeamAssociationFullAccess | 541 |
| 使用此策略 | 541 |
| 策略详细信息 | 541 |
| 策略版本 | 542 |
| JSON 策略文档 | 542 |
| 了解更多信息 | 542 |
| AmazonHoneycodeTeamAssociationReadOnlyAccess | 542 |
| 使用此策略 | 542 |
| 策略详细信息 | 543 |
| 策略版本 | 543 |
| JSON 策略文档 | 543 |
| 了解更多信息 | 543 |

| | |
|--|-----|
| AmazonHoneycodeWorkbookFullAccess | 544 |
| 使用此策略 | 544 |
| 策略详细信息 | 544 |
| 策略版本 | 544 |
| JSON 策略文档 | 544 |
| 了解更多信息 | 545 |
| AmazonHoneycodeWorkbookReadOnlyAccess | 545 |
| 使用此策略 | 545 |
| 策略详细信息 | 545 |
| 策略版本 | 545 |
| JSON 策略文档 | 546 |
| 了解更多信息 | 546 |
| AmazonInspector2AgentlessServiceRolePolicy | 546 |
| 使用此策略 | 546 |
| 策略详细信息 | 546 |
| 策略版本 | 547 |
| JSON 策略文档 | 547 |
| 了解更多信息 | 550 |
| AmazonInspector2FullAccess | 551 |
| 使用此策略 | 551 |
| 策略详细信息 | 551 |
| 策略版本 | 551 |
| JSON 策略文档 | 551 |
| 了解更多信息 | 552 |
| AmazonInspector2ManagedCisPolicy | 552 |
| 使用此策略 | 553 |
| 策略详细信息 | 553 |
| 策略版本 | 553 |
| JSON 策略文档 | 553 |
| 了解更多信息 | 553 |
| AmazonInspector2ReadOnlyAccess | 554 |
| 使用此策略 | 554 |
| 策略详细信息 | 554 |
| 策略版本 | 554 |
| JSON 策略文档 | 554 |
| 了解更多信息 | 555 |

| | |
|---|-----|
| AmazonInspector2ServiceRolePolicy | 555 |
| 使用此策略 | 555 |
| 策略详细信息 | 555 |
| 策略版本 | 556 |
| JSON 策略文档 | 556 |
| 了解更多信息 | 562 |
| AmazonInspectorFullAccess | 562 |
| 使用此策略 | 562 |
| 策略详细信息 | 562 |
| 策略版本 | 563 |
| JSON 策略文档 | 563 |
| 了解更多信息 | 564 |
| AmazonInspectorReadOnlyAccess | 564 |
| 使用此策略 | 564 |
| 策略详细信息 | 564 |
| 策略版本 | 565 |
| JSON 策略文档 | 565 |
| 了解更多信息 | 565 |
| AmazonInspectorServiceRolePolicy | 566 |
| 使用此策略 | 566 |
| 策略详细信息 | 566 |
| 策略版本 | 566 |
| JSON 策略文档 | 566 |
| 了解更多信息 | 567 |
| AmazonKendraFullAccess | 568 |
| 使用此策略 | 568 |
| 策略详细信息 | 568 |
| 策略版本 | 568 |
| JSON 策略文档 | 568 |
| 了解更多信息 | 570 |
| AmazonKendraReadOnlyAccess | 570 |
| 使用此策略 | 570 |
| 策略详细信息 | 570 |
| 策略版本 | 571 |
| JSON 策略文档 | 571 |
| 了解更多信息 | 571 |

| | |
|--|-----|
| AmazonKeyspacesFullAccess | 572 |
| 使用此策略 | 572 |
| 策略详细信息 | 572 |
| 策略版本 | 572 |
| JSON 策略文档 | 572 |
| 了解更多信息 | 574 |
| AmazonKeyspacesReadOnlyAccess | 574 |
| 使用此策略 | 574 |
| 策略详细信息 | 574 |
| 策略版本 | 575 |
| JSON 策略文档 | 575 |
| 了解更多信息 | 575 |
| AmazonKeyspacesReadOnlyAccess_v2 | 576 |
| 使用此策略 | 576 |
| 策略详细信息 | 576 |
| 策略版本 | 576 |
| JSON 策略文档 | 576 |
| 了解更多信息 | 577 |
| AmazonKinesisAnalyticsFullAccess | 577 |
| 使用此策略 | 578 |
| 策略详细信息 | 578 |
| 策略版本 | 578 |
| JSON 策略文档 | 578 |
| 了解更多信息 | 579 |
| AmazonKinesisAnalyticsReadOnly | 580 |
| 使用此策略 | 580 |
| 策略详细信息 | 580 |
| 策略版本 | 580 |
| JSON 策略文档 | 580 |
| 了解更多信息 | 581 |
| AmazonKinesisFirehoseFullAccess | 582 |
| 使用此策略 | 582 |
| 策略详细信息 | 582 |
| 策略版本 | 582 |
| JSON 策略文档 | 582 |
| 了解更多信息 | 583 |

| | |
|---|-----|
| AmazonKinesisFirehoseReadOnlyAccess | 583 |
| 使用此策略 | 583 |
| 策略详细信息 | 583 |
| 策略版本 | 583 |
| JSON 策略文档 | 584 |
| 了解更多信息 | 584 |
| AmazonKinesisFullAccess | 584 |
| 使用此策略 | 584 |
| 策略详细信息 | 584 |
| 策略版本 | 585 |
| JSON 策略文档 | 585 |
| 了解更多信息 | 585 |
| AmazonKinesisReadOnlyAccess | 585 |
| 使用此策略 | 585 |
| 策略详细信息 | 586 |
| 策略版本 | 586 |
| JSON 策略文档 | 586 |
| 了解更多信息 | 586 |
| AmazonKinesisVideoStreamsFullAccess | 587 |
| 使用此策略 | 587 |
| 策略详细信息 | 587 |
| 策略版本 | 587 |
| JSON 策略文档 | 587 |
| 了解更多信息 | 587 |
| AmazonKinesisVideoStreamsReadOnlyAccess | 588 |
| 使用此策略 | 588 |
| 策略详细信息 | 588 |
| 策略版本 | 588 |
| JSON 策略文档 | 588 |
| 了解更多信息 | 589 |
| AmazonLaunchWizard_Fullaccess | 589 |
| 使用此策略 | 589 |
| 策略详细信息 | 589 |
| 策略版本 | 589 |
| JSON 策略文档 | 590 |
| 了解更多信息 | 604 |

| | |
|--------------------------------------|-----|
| AmazonLaunchWizardFullAccessV2 | 604 |
| 使用此策略 | 604 |
| 策略详细信息 | 604 |
| 策略版本 | 604 |
| JSON 策略文档 | 605 |
| 了解更多信息 | 621 |
| AmazonLexChannelsAccess | 621 |
| 使用此策略 | 621 |
| 策略详细信息 | 621 |
| 策略版本 | 622 |
| JSON 策略文档 | 622 |
| 了解更多信息 | 622 |
| AmazonLexFullAccess | 622 |
| 使用此策略 | 622 |
| 策略详细信息 | 623 |
| 策略版本 | 623 |
| JSON 策略文档 | 623 |
| 了解更多信息 | 628 |
| AmazonLexReadOnly | 629 |
| 使用此策略 | 629 |
| 策略详细信息 | 629 |
| 策略版本 | 629 |
| JSON 策略文档 | 629 |
| 了解更多信息 | 631 |
| AmazonLexReplicationPolicy | 631 |
| 使用此策略 | 631 |
| 策略详细信息 | 631 |
| 策略版本 | 631 |
| JSON 策略文档 | 631 |
| 了解更多信息 | 634 |
| AmazonLexRunBotsOnly | 634 |
| 使用此策略 | 634 |
| 策略详细信息 | 634 |
| 策略版本 | 634 |
| JSON 策略文档 | 634 |
| 了解更多信息 | 635 |

| | |
|--|-----|
| AmazonLexV2BotPolicy | 635 |
| 使用此策略 | 635 |
| 策略详细信息 | 635 |
| 策略版本 | 635 |
| JSON 策略文档 | 636 |
| 了解更多信息 | 636 |
| AmazonLookoutEquipmentFullAccess | 636 |
| 使用此策略 | 636 |
| 策略详细信息 | 636 |
| 策略版本 | 637 |
| JSON 策略文档 | 637 |
| 了解更多信息 | 638 |
| AmazonLookoutEquipmentReadOnlyAccess | 638 |
| 使用此策略 | 638 |
| 策略详细信息 | 638 |
| 策略版本 | 639 |
| JSON 策略文档 | 639 |
| 了解更多信息 | 639 |
| AmazonLookoutMetricsFullAccess | 639 |
| 使用此策略 | 639 |
| 策略详细信息 | 640 |
| 策略版本 | 640 |
| JSON 策略文档 | 640 |
| 了解更多信息 | 641 |
| AmazonLookoutMetricsReadOnlyAccess | 641 |
| 使用此策略 | 641 |
| 策略详细信息 | 641 |
| 策略版本 | 641 |
| JSON 策略文档 | 641 |
| 了解更多信息 | 642 |
| AmazonLookoutVisionConsoleFullAccess | 642 |
| 使用此策略 | 642 |
| 策略详细信息 | 643 |
| 策略版本 | 643 |
| JSON 策略文档 | 643 |
| 了解更多信息 | 645 |

| | |
|---|-----|
| AmazonLookoutVisionConsoleReadOnlyAccess | 645 |
| 使用此策略 | 645 |
| 策略详细信息 | 646 |
| 策略版本 | 646 |
| JSON 策略文档 | 646 |
| 了解更多信息 | 647 |
| AmazonLookoutVisionFullAccess | 647 |
| 使用此策略 | 647 |
| 策略详细信息 | 648 |
| 策略版本 | 648 |
| JSON 策略文档 | 648 |
| 了解更多信息 | 648 |
| AmazonLookoutVisionReadOnlyAccess | 649 |
| 使用此策略 | 649 |
| 策略详细信息 | 649 |
| 策略版本 | 649 |
| JSON 策略文档 | 649 |
| 了解更多信息 | 650 |
| AmazonMachineLearningBatchPredictionsAccess | 650 |
| 使用此策略 | 650 |
| 策略详细信息 | 650 |
| 策略版本 | 650 |
| JSON 策略文档 | 651 |
| 了解更多信息 | 651 |
| AmazonMachineLearningCreateOnlyAccess | 651 |
| 使用此策略 | 651 |
| 策略详细信息 | 651 |
| 策略版本 | 652 |
| JSON 策略文档 | 652 |
| 了解更多信息 | 652 |
| AmazonMachineLearningFullAccess | 653 |
| 使用此策略 | 653 |
| 策略详细信息 | 653 |
| 策略版本 | 653 |
| JSON 策略文档 | 653 |
| 了解更多信息 | 654 |

| | |
|---|-----|
| AmazonMachineLearningManageRealTimeEndpointOnlyAccess | 654 |
| 使用此策略 | 654 |
| 策略详细信息 | 654 |
| 策略版本 | 654 |
| JSON 策略文档 | 654 |
| 了解更多信息 | 655 |
| AmazonMachineLearningReadOnlyAccess | 655 |
| 使用此策略 | 655 |
| 策略详细信息 | 655 |
| 策略版本 | 655 |
| JSON 策略文档 | 656 |
| 了解更多信息 | 656 |
| AmazonMachineLearningRealTimePredictionOnlyAccess | 656 |
| 使用此策略 | 656 |
| 策略详细信息 | 656 |
| 策略版本 | 657 |
| JSON 策略文档 | 657 |
| 了解更多信息 | 657 |
| AmazonMachineLearningRoleforRedshiftDataSourceV3 | 657 |
| 使用此策略 | 658 |
| 策略详细信息 | 658 |
| 策略版本 | 658 |
| JSON 策略文档 | 658 |
| 了解更多信息 | 659 |
| AmazonMacieFullAccess | 659 |
| 使用此策略 | 659 |
| 策略详细信息 | 659 |
| 策略版本 | 660 |
| JSON 策略文档 | 660 |
| 了解更多信息 | 660 |
| AmazonMacieHandshakeRole | 661 |
| 使用此策略 | 661 |
| 策略详细信息 | 661 |
| 策略版本 | 661 |
| JSON 策略文档 | 661 |
| 了解更多信息 | 662 |

| | |
|--|-----|
| AmazonMacieReadOnlyAccess | 662 |
| 使用此策略 | 662 |
| 策略详细信息 | 662 |
| 策略版本 | 662 |
| JSON 策略文档 | 662 |
| 了解更多信息 | 663 |
| AmazonMacieServiceRole | 663 |
| 使用此策略 | 663 |
| 策略详细信息 | 663 |
| 策略版本 | 664 |
| JSON 策略文档 | 664 |
| 了解更多信息 | 664 |
| AmazonMacieServiceRolePolicy | 664 |
| 使用此策略 | 664 |
| 策略详细信息 | 665 |
| 策略版本 | 665 |
| JSON 策略文档 | 665 |
| 了解更多信息 | 666 |
| AmazonManagedBlockchainConsoleFullAccess | 666 |
| 使用此策略 | 667 |
| 策略详细信息 | 667 |
| 策略版本 | 667 |
| JSON 策略文档 | 667 |
| 了解更多信息 | 668 |
| AmazonManagedBlockchainFullAccess | 668 |
| 使用此策略 | 668 |
| 策略详细信息 | 668 |
| 策略版本 | 668 |
| JSON 策略文档 | 668 |
| 了解更多信息 | 669 |
| AmazonManagedBlockchainReadOnlyAccess | 669 |
| 使用此策略 | 669 |
| 策略详细信息 | 669 |
| 策略版本 | 669 |
| JSON 策略文档 | 670 |
| 了解更多信息 | 670 |

| | |
|--|-----|
| AmazonManagedBlockchainServiceRolePolicy | 670 |
| 使用此策略 | 670 |
| 策略详细信息 | 671 |
| 策略版本 | 671 |
| JSON 策略文档 | 671 |
| 了解更多信息 | 672 |
| AmazonMCSFullAccess | 672 |
| 使用此策略 | 672 |
| 策略详细信息 | 672 |
| 策略版本 | 672 |
| JSON 策略文档 | 672 |
| 了解更多信息 | 674 |
| AmazonMCSReadOnlyAccess | 674 |
| 使用此策略 | 674 |
| 策略详细信息 | 674 |
| 策略版本 | 674 |
| JSON 策略文档 | 674 |
| 了解更多信息 | 675 |
| AmazonMechanicalTurkFullAccess | 675 |
| 使用此策略 | 675 |
| 策略详细信息 | 675 |
| 策略版本 | 676 |
| JSON 策略文档 | 676 |
| 了解更多信息 | 676 |
| AmazonMechanicalTurkReadOnly | 676 |
| 使用此策略 | 677 |
| 策略详细信息 | 677 |
| 策略版本 | 677 |
| JSON 策略文档 | 677 |
| 了解更多信息 | 677 |
| AmazonMemoryDBFullAccess | 678 |
| 使用此策略 | 678 |
| 策略详细信息 | 678 |
| 策略版本 | 678 |
| JSON 策略文档 | 678 |
| 了解更多信息 | 679 |

| | |
|--|-----|
| AmazonMemoryDBReadOnlyAccess | 679 |
| 使用此策略 | 679 |
| 策略详细信息 | 679 |
| 策略版本 | 680 |
| JSON 策略文档 | 680 |
| 了解更多信息 | 680 |
| AmazonMobileAnalyticsFinancialReportAccess | 680 |
| 使用此策略 | 680 |
| 策略详细信息 | 681 |
| 策略版本 | 681 |
| JSON 策略文档 | 681 |
| 了解更多信息 | 681 |
| AmazonMobileAnalyticsFullAccess | 682 |
| 使用此策略 | 682 |
| 策略详细信息 | 682 |
| 策略版本 | 682 |
| JSON 策略文档 | 682 |
| 了解更多信息 | 682 |
| AmazonMobileAnalyticsNon-financialReportAccess | 683 |
| 使用此策略 | 683 |
| 策略详细信息 | 683 |
| 策略版本 | 683 |
| JSON 策略文档 | 683 |
| 了解更多信息 | 684 |
| AmazonMobileAnalyticsWriteOnlyAccess | 684 |
| 使用此策略 | 684 |
| 策略详细信息 | 684 |
| 策略版本 | 684 |
| JSON 策略文档 | 684 |
| 了解更多信息 | 685 |
| AmazonMonitronFullAccess | 685 |
| 使用此策略 | 685 |
| 策略详细信息 | 685 |
| 策略版本 | 685 |
| JSON 策略文档 | 686 |
| 了解更多信息 | 687 |

| | |
|--------------------------------------|-----|
| AmazonMQApiFullAccess | 688 |
| 使用此策略 | 688 |
| 策略详细信息 | 688 |
| 策略版本 | 688 |
| JSON 策略文档 | 688 |
| 了解更多信息 | 689 |
| AmazonMQApiReadOnlyAccess | 689 |
| 使用此策略 | 690 |
| 策略详细信息 | 690 |
| 策略版本 | 690 |
| JSON 策略文档 | 690 |
| 了解更多信息 | 691 |
| AmazonMQFullAccess | 691 |
| 使用此策略 | 691 |
| 策略详细信息 | 691 |
| 策略版本 | 691 |
| JSON 策略文档 | 691 |
| 了解更多信息 | 693 |
| AmazonMQReadOnlyAccess | 693 |
| 使用此策略 | 693 |
| 策略详细信息 | 693 |
| 策略版本 | 693 |
| JSON 策略文档 | 693 |
| 了解更多信息 | 694 |
| AmazonMQServiceRolePolicy | 694 |
| 使用此策略 | 694 |
| 策略详细信息 | 694 |
| 策略版本 | 694 |
| JSON 策略文档 | 695 |
| 了解更多信息 | 696 |
| AmazonMSKConnectReadOnlyAccess | 697 |
| 使用此策略 | 697 |
| 策略详细信息 | 697 |
| 策略版本 | 697 |
| JSON 策略文档 | 697 |
| 了解更多信息 | 698 |

| | |
|--|-----|
| AmazonMSKFullAccess | 698 |
| 使用此策略 | 699 |
| 策略详细信息 | 699 |
| 策略版本 | 699 |
| JSON 策略文档 | 699 |
| 了解更多信息 | 702 |
| AmazonMSKReadOnlyAccess | 702 |
| 使用此策略 | 702 |
| 策略详细信息 | 702 |
| 策略版本 | 702 |
| JSON 策略文档 | 703 |
| 了解更多信息 | 703 |
| AmazonMWAAServiceRolePolicy | 703 |
| 使用此策略 | 704 |
| 策略详细信息 | 704 |
| 策略版本 | 704 |
| JSON 策略文档 | 704 |
| 了解更多信息 | 706 |
| AmazonNimbleStudio-LaunchProfileWorker | 706 |
| 使用此策略 | 707 |
| 策略详细信息 | 707 |
| 策略版本 | 707 |
| JSON 策略文档 | 707 |
| 了解更多信息 | 708 |
| AmazonNimbleStudio-StudioAdmin | 708 |
| 使用此策略 | 708 |
| 策略详细信息 | 708 |
| 策略版本 | 708 |
| JSON 策略文档 | 709 |
| 了解更多信息 | 710 |
| AmazonNimbleStudio-StudioUser | 711 |
| 使用此策略 | 711 |
| 策略详细信息 | 711 |
| 策略版本 | 711 |
| JSON 策略文档 | 711 |
| 了解更多信息 | 713 |

| | |
|---|-----|
| AmazonOmicsFullAccess | 713 |
| 使用此策略 | 714 |
| 策略详细信息 | 714 |
| 策略版本 | 714 |
| JSON 策略文档 | 714 |
| 了解更多信息 | 715 |
| AmazonOmicsReadOnlyAccess | 715 |
| 使用此策略 | 715 |
| 策略详细信息 | 715 |
| 策略版本 | 716 |
| JSON 策略文档 | 716 |
| 了解更多信息 | 716 |
| AmazonOneEnterpriseFullAccess | 716 |
| 使用此策略 | 716 |
| 策略详细信息 | 717 |
| 策略版本 | 717 |
| JSON 策略文档 | 717 |
| 了解更多信息 | 717 |
| AmazonOneEnterpriseInstallerAccess | 718 |
| 使用此策略 | 718 |
| 策略详细信息 | 718 |
| 策略版本 | 718 |
| JSON 策略文档 | 718 |
| 了解更多信息 | 719 |
| AmazonOneEnterpriseReadOnlyAccess | 719 |
| 使用此策略 | 719 |
| 策略详细信息 | 719 |
| 策略版本 | 719 |
| JSON 策略文档 | 719 |
| 了解更多信息 | 720 |
| AmazonOpenSearchDashboardsServiceRolePolicy | 720 |
| 使用此策略 | 720 |
| 策略详细信息 | 720 |
| 策略版本 | 721 |
| JSON 策略文档 | 721 |
| 了解更多信息 | 721 |

| | |
|---|-----|
| AmazonOpenSearchIngestionFullAccess | 721 |
| 使用此策略 | 721 |
| 策略详细信息 | 722 |
| 策略版本 | 722 |
| JSON 策略文档 | 722 |
| 了解更多信息 | 723 |
| AmazonOpenSearchIngestionReadOnlyAccess | 723 |
| 使用此策略 | 723 |
| 策略详细信息 | 723 |
| 策略版本 | 723 |
| JSON 策略文档 | 724 |
| 了解更多信息 | 724 |
| AmazonOpenSearchIngestionServiceRolePolicy | 724 |
| 使用此策略 | 724 |
| 策略详细信息 | 725 |
| 策略版本 | 725 |
| JSON 策略文档 | 725 |
| 了解更多信息 | 727 |
| AmazonOpenSearchServerlessServiceRolePolicy | 727 |
| 使用此策略 | 727 |
| 策略详细信息 | 727 |
| 策略版本 | 727 |
| JSON 策略文档 | 728 |
| 了解更多信息 | 728 |
| AmazonOpenSearchServiceCognitoAccess | 728 |
| 使用此策略 | 728 |
| 策略详细信息 | 728 |
| 策略版本 | 729 |
| JSON 策略文档 | 729 |
| 了解更多信息 | 730 |
| AmazonOpenSearchServiceFullAccess | 730 |
| 使用此策略 | 730 |
| 策略详细信息 | 730 |
| 策略版本 | 730 |
| JSON 策略文档 | 731 |
| 了解更多信息 | 731 |

| | |
|---|-----|
| AmazonOpenSearchServiceReadOnlyAccess | 731 |
| 使用此策略 | 731 |
| 策略详细信息 | 731 |
| 策略版本 | 732 |
| JSON 策略文档 | 732 |
| 了解更多信息 | 732 |
| AmazonOpenSearchServiceRolePolicy | 732 |
| 使用此策略 | 733 |
| 策略详细信息 | 733 |
| 策略版本 | 733 |
| JSON 策略文档 | 733 |
| 了解更多信息 | 738 |
| AmazonPersonalizeFullAccess | 738 |
| 使用此策略 | 738 |
| 策略详细信息 | 738 |
| 策略版本 | 738 |
| JSON 策略文档 | 738 |
| 了解更多信息 | 739 |
| AmazonPollyFullAccess | 740 |
| 使用此策略 | 740 |
| 策略详细信息 | 740 |
| 策略版本 | 740 |
| JSON 策略文档 | 740 |
| 了解更多信息 | 741 |
| AmazonPollyReadOnlyAccess | 741 |
| 使用此策略 | 741 |
| 策略详细信息 | 741 |
| 策略版本 | 741 |
| JSON 策略文档 | 741 |
| 了解更多信息 | 742 |
| AmazonPrometheusConsoleFullAccess | 742 |
| 使用此策略 | 742 |
| 策略详细信息 | 742 |
| 策略版本 | 743 |
| JSON 策略文档 | 743 |
| 了解更多信息 | 744 |

| | |
|--|-----|
| AmazonPrometheusFullAccess | 744 |
| 使用此策略 | 744 |
| 策略详细信息 | 744 |
| 策略版本 | 744 |
| JSON 策略文档 | 745 |
| 了解更多信息 | 746 |
| AmazonPrometheusQueryAccess | 746 |
| 使用此策略 | 746 |
| 策略详细信息 | 746 |
| 策略版本 | 746 |
| JSON 策略文档 | 747 |
| 了解更多信息 | 747 |
| AmazonPrometheusRemoteWriteAccess | 747 |
| 使用此策略 | 747 |
| 策略详细信息 | 747 |
| 策略版本 | 748 |
| JSON 策略文档 | 748 |
| 了解更多信息 | 748 |
| AmazonPrometheusScraperServiceRolePolicy | 748 |
| 使用此策略 | 749 |
| 策略详细信息 | 749 |
| 策略版本 | 749 |
| JSON 策略文档 | 749 |
| 了解更多信息 | 751 |
| AmazonQFullAccess | 751 |
| 使用此策略 | 751 |
| 策略详细信息 | 751 |
| 策略版本 | 752 |
| JSON 策略文档 | 752 |
| 了解更多信息 | 752 |
| AmazonQLDBConsoleFullAccess | 752 |
| 使用此策略 | 752 |
| 策略详细信息 | 753 |
| 策略版本 | 753 |
| JSON 策略文档 | 753 |
| 了解更多信息 | 755 |

| | |
|--|-----|
| AmazonQLDBFullAccess | 755 |
| 使用此策略 | 755 |
| 策略详细信息 | 755 |
| 策略版本 | 755 |
| JSON 策略文档 | 755 |
| 了解更多信息 | 757 |
| AmazonQLDBReadOnly | 757 |
| 使用此策略 | 757 |
| 策略详细信息 | 757 |
| 策略版本 | 757 |
| JSON 策略文档 | 758 |
| 了解更多信息 | 758 |
| AmazonRDSBetaServiceRolePolicy | 758 |
| 使用此策略 | 758 |
| 策略详细信息 | 759 |
| 策略版本 | 759 |
| JSON 策略文档 | 759 |
| 了解更多信息 | 762 |
| AmazonRDSCustomInstanceProfileRolePolicy | 762 |
| 使用此策略 | 762 |
| 策略详细信息 | 762 |
| 策略版本 | 763 |
| JSON 策略文档 | 763 |
| 了解更多信息 | 770 |
| AmazonRDSCustomPreviewServiceRolePolicy | 770 |
| 使用此策略 | 770 |
| 策略详细信息 | 770 |
| 策略版本 | 771 |
| JSON 策略文档 | 771 |
| 了解更多信息 | 786 |
| AmazonRDSCustomServiceRolePolicy | 786 |
| 使用此策略 | 787 |
| 策略详细信息 | 787 |
| 策略版本 | 787 |
| JSON 策略文档 | 787 |
| 了解更多信息 | 804 |

| | |
|--|-----|
| AmazonRDSDataFullAccess | 804 |
| 使用此策略 | 804 |
| 策略详细信息 | 804 |
| 策略版本 | 804 |
| JSON 策略文档 | 805 |
| 了解更多信息 | 806 |
| AmazonRDSDirectoryServiceAccess | 806 |
| 使用此策略 | 806 |
| 策略详细信息 | 806 |
| 策略版本 | 806 |
| JSON 策略文档 | 806 |
| 了解更多信息 | 807 |
| AmazonRDSEnhancedMonitoringRole | 807 |
| 使用此策略 | 807 |
| 策略详细信息 | 807 |
| 策略版本 | 808 |
| JSON 策略文档 | 808 |
| 了解更多信息 | 808 |
| AmazonRDSFullAccess | 809 |
| 使用此策略 | 809 |
| 策略详细信息 | 809 |
| 策略版本 | 809 |
| JSON 策略文档 | 809 |
| 了解更多信息 | 811 |
| AmazonRDSPerformanceInsightsFullAccess | 812 |
| 使用此策略 | 812 |
| 策略详细信息 | 812 |
| 策略版本 | 812 |
| JSON 策略文档 | 812 |
| 了解更多信息 | 814 |
| AmazonRDSPerformanceInsightsReadOnly | 814 |
| 使用此策略 | 814 |
| 策略详细信息 | 814 |
| 策略版本 | 814 |
| JSON 策略文档 | 814 |
| 了解更多信息 | 816 |

| | |
|---|-----|
| AmazonRDSPreviewServiceRolePolicy | 816 |
| 使用此策略 | 816 |
| 策略详细信息 | 817 |
| 策略版本 | 817 |
| JSON 策略文档 | 817 |
| 了解更多信息 | 820 |
| AmazonRDSReadOnlyAccess | 820 |
| 使用此策略 | 820 |
| 策略详细信息 | 821 |
| 策略版本 | 821 |
| JSON 策略文档 | 821 |
| 了解更多信息 | 822 |
| AmazonRDSServiceRolePolicy | 822 |
| 使用此策略 | 823 |
| 策略详细信息 | 823 |
| 策略版本 | 823 |
| JSON 策略文档 | 823 |
| 了解更多信息 | 827 |
| AmazonRedshiftAllCommandsFullAccess | 827 |
| 使用此策略 | 827 |
| 策略详细信息 | 827 |
| 策略版本 | 828 |
| JSON 策略文档 | 828 |
| 了解更多信息 | 833 |
| AmazonRedshiftDataFullAccess | 833 |
| 使用此策略 | 833 |
| 策略详细信息 | 833 |
| 策略版本 | 834 |
| JSON 策略文档 | 834 |
| 了解更多信息 | 836 |
| AmazonRedshiftFullAccess | 836 |
| 使用此策略 | 836 |
| 策略详细信息 | 836 |
| 策略版本 | 836 |
| JSON 策略文档 | 836 |
| 了解更多信息 | 838 |

| | |
|---|-----|
| AmazonRedshiftQueryEditor | 839 |
| 使用此策略 | 839 |
| 策略详细信息 | 839 |
| 策略版本 | 839 |
| JSON 策略文档 | 839 |
| 了解更多信息 | 841 |
| AmazonRedshiftQueryEditorV2FullAccess | 841 |
| 使用此策略 | 842 |
| 策略详细信息 | 842 |
| 策略版本 | 842 |
| JSON 策略文档 | 842 |
| 了解更多信息 | 843 |
| AmazonRedshiftQueryEditorV2NoSharing | 844 |
| 使用此策略 | 844 |
| 策略详细信息 | 844 |
| 策略版本 | 844 |
| JSON 策略文档 | 844 |
| 了解更多信息 | 848 |
| AmazonRedshiftQueryEditorV2ReadSharing | 848 |
| 使用此策略 | 848 |
| 策略详细信息 | 848 |
| 策略版本 | 849 |
| JSON 策略文档 | 849 |
| 了解更多信息 | 854 |
| AmazonRedshiftQueryEditorV2ReadWriteSharing | 854 |
| 使用此策略 | 854 |
| 策略详细信息 | 854 |
| 策略版本 | 854 |
| JSON 策略文档 | 854 |
| 了解更多信息 | 859 |
| AmazonRedshiftReadOnlyAccess | 860 |
| 使用此策略 | 860 |
| 策略详细信息 | 860 |
| 策略版本 | 860 |
| JSON 策略文档 | 860 |
| 了解更多信息 | 861 |

| | |
|---|-----|
| AmazonRedshiftServiceLinkedRolePolicy | 861 |
| 使用此策略 | 861 |
| 策略详细信息 | 861 |
| 策略版本 | 862 |
| JSON 策略文档 | 862 |
| 了解更多信息 | 867 |
| AmazonRekognitionCustomLabelsFullAccess | 867 |
| 使用此策略 | 867 |
| 策略详细信息 | 867 |
| 策略版本 | 868 |
| JSON 策略文档 | 868 |
| 了解更多信息 | 869 |
| AmazonRekognitionFullAccess | 869 |
| 使用此策略 | 869 |
| 策略详细信息 | 869 |
| 策略版本 | 870 |
| JSON 策略文档 | 870 |
| 了解更多信息 | 870 |
| AmazonRekognitionReadOnlyAccess | 870 |
| 使用此策略 | 871 |
| 策略详细信息 | 871 |
| 策略版本 | 871 |
| JSON 策略文档 | 871 |
| 了解更多信息 | 872 |
| AmazonRekognitionServiceRole | 872 |
| 使用此策略 | 873 |
| 策略详细信息 | 873 |
| 策略版本 | 873 |
| JSON 策略文档 | 873 |
| 了解更多信息 | 874 |
| AmazonRoute53AutoNamingFullAccess | 874 |
| 使用此策略 | 874 |
| 策略详细信息 | 874 |
| 策略版本 | 874 |
| JSON 策略文档 | 875 |
| 了解更多信息 | 875 |

| | |
|---|-----|
| AmazonRoute53AutoNamingReadOnlyAccess | 875 |
| 使用此策略 | 876 |
| 策略详细信息 | 876 |
| 策略版本 | 876 |
| JSON 策略文档 | 876 |
| 了解更多信息 | 876 |
| AmazonRoute53AutoNamingRegistrantAccess | 877 |
| 使用此策略 | 877 |
| 策略详细信息 | 877 |
| 策略版本 | 877 |
| JSON 策略文档 | 877 |
| 了解更多信息 | 878 |
| AmazonRoute53DomainsFullAccess | 878 |
| 使用此策略 | 878 |
| 策略详细信息 | 878 |
| 策略版本 | 879 |
| JSON 策略文档 | 879 |
| 了解更多信息 | 879 |
| AmazonRoute53DomainsReadOnlyAccess | 879 |
| 使用此策略 | 880 |
| 策略详细信息 | 880 |
| 策略版本 | 880 |
| JSON 策略文档 | 880 |
| 了解更多信息 | 880 |
| AmazonRoute53FullAccess | 881 |
| 使用此策略 | 881 |
| 策略详细信息 | 881 |
| 策略版本 | 881 |
| JSON 策略文档 | 881 |
| 了解更多信息 | 882 |
| AmazonRoute53ReadOnlyAccess | 882 |
| 使用此策略 | 882 |
| 策略详细信息 | 883 |
| 策略版本 | 883 |
| JSON 策略文档 | 883 |
| 了解更多信息 | 883 |

| | |
|--|-----|
| AmazonRoute53RecoveryClusterFullAccess | 884 |
| 使用此策略 | 884 |
| 策略详细信息 | 884 |
| 策略版本 | 884 |
| JSON 策略文档 | 884 |
| 了解更多信息 | 885 |
| AmazonRoute53RecoveryClusterReadOnlyAccess | 885 |
| 使用此策略 | 885 |
| 策略详细信息 | 885 |
| 策略版本 | 885 |
| JSON 策略文档 | 885 |
| 了解更多信息 | 886 |
| AmazonRoute53RecoveryControlConfigFullAccess | 886 |
| 使用此策略 | 886 |
| 策略详细信息 | 886 |
| 策略版本 | 886 |
| JSON 策略文档 | 887 |
| 了解更多信息 | 887 |
| AmazonRoute53RecoveryControlConfigReadOnlyAccess | 887 |
| 使用此策略 | 887 |
| 策略详细信息 | 887 |
| 策略版本 | 888 |
| JSON 策略文档 | 888 |
| 了解更多信息 | 888 |
| AmazonRoute53RecoveryReadinessFullAccess | 889 |
| 使用此策略 | 889 |
| 策略详细信息 | 889 |
| 策略版本 | 889 |
| JSON 策略文档 | 889 |
| 了解更多信息 | 890 |
| AmazonRoute53RecoveryReadinessReadOnlyAccess | 890 |
| 使用此策略 | 890 |
| 策略详细信息 | 890 |
| 策略版本 | 890 |
| JSON 策略文档 | 891 |
| 了解更多信息 | 891 |

| | |
|---|-----|
| AmazonRoute53ResolverFullAccess | 892 |
| 使用此策略 | 892 |
| 策略详细信息 | 892 |
| 策略版本 | 892 |
| JSON 策略文档 | 892 |
| 了解更多信息 | 893 |
| AmazonRoute53ResolverReadOnlyAccess | 893 |
| 使用此策略 | 893 |
| 策略详细信息 | 893 |
| 策略版本 | 893 |
| JSON 策略文档 | 894 |
| 了解更多信息 | 894 |
| AmazonS3FullAccess | 894 |
| 使用此策略 | 895 |
| 策略详细信息 | 895 |
| 策略版本 | 895 |
| JSON 策略文档 | 895 |
| 了解更多信息 | 895 |
| AmazonS3ObjectLambdaExecutionRolePolicy | 896 |
| 使用此策略 | 896 |
| 策略详细信息 | 896 |
| 策略版本 | 896 |
| JSON 策略文档 | 896 |
| 了解更多信息 | 897 |
| AmazonS3OutpostsFullAccess | 897 |
| 使用此策略 | 897 |
| 策略详细信息 | 897 |
| 策略版本 | 897 |
| JSON 策略文档 | 898 |
| 了解更多信息 | 899 |
| AmazonS3OutpostsReadOnlyAccess | 899 |
| 使用此策略 | 899 |
| 策略详细信息 | 899 |
| 策略版本 | 899 |
| JSON 策略文档 | 899 |
| 了解更多信息 | 900 |

| | |
|--|-----|
| AmazonS3ReadOnlyAccess | 901 |
| 使用此策略 | 901 |
| 策略详细信息 | 901 |
| 策略版本 | 901 |
| JSON 策略文档 | 901 |
| 了解更多信息 | 902 |
| AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy | 902 |
| 使用此策略 | 902 |
| 策略详细信息 | 902 |
| 策略版本 | 903 |
| JSON 策略文档 | 903 |
| 了解更多信息 | 913 |
| AmazonSageMakerCanvasAIServicesAccess | 913 |
| 使用此策略 | 913 |
| 策略详细信息 | 913 |
| 策略版本 | 913 |
| JSON 策略文档 | 913 |
| 了解更多信息 | 916 |
| AmazonSageMakerCanvasBedrockAccess | 917 |
| 使用此策略 | 917 |
| 策略详细信息 | 917 |
| 策略版本 | 917 |
| JSON 策略文档 | 917 |
| 了解更多信息 | 918 |
| AmazonSageMakerCanvasDataPrepFullAccess | 918 |
| 使用此策略 | 918 |
| 策略详细信息 | 918 |
| 策略版本 | 919 |
| JSON 策略文档 | 919 |
| 了解更多信息 | 926 |
| AmazonSageMakerCanvasDirectDeployAccess | 926 |
| 使用此策略 | 926 |
| 策略详细信息 | 926 |
| 策略版本 | 927 |
| JSON 策略文档 | 927 |
| 了解更多信息 | 927 |

| | |
|--|-----|
| AmazonSageMakerCanvasForecastAccess | 928 |
| 使用此策略 | 928 |
| 策略详细信息 | 928 |
| 策略版本 | 928 |
| JSON 策略文档 | 928 |
| 了解更多信息 | 929 |
| AmazonSageMakerCanvasFullAccess | 929 |
| 使用此策略 | 929 |
| 策略详细信息 | 929 |
| 策略版本 | 930 |
| JSON 策略文档 | 930 |
| 了解更多信息 | 938 |
| AmazonSageMakerClusterInstanceRolePolicy | 938 |
| 使用此策略 | 938 |
| 策略详细信息 | 938 |
| 策略版本 | 938 |
| JSON 策略文档 | 939 |
| 了解更多信息 | 940 |
| AmazonSageMakerCoreServiceRolePolicy | 940 |
| 使用此策略 | 941 |
| 策略详细信息 | 941 |
| 策略版本 | 941 |
| JSON 策略文档 | 941 |
| 了解更多信息 | 942 |
| AmazonSageMakerEdgeDeviceFleetPolicy | 942 |
| 使用此策略 | 942 |
| 策略详细信息 | 942 |
| 策略版本 | 943 |
| JSON 策略文档 | 943 |
| 了解更多信息 | 945 |
| AmazonSageMakerFeatureStoreAccess | 945 |
| 使用此策略 | 945 |
| 策略详细信息 | 945 |
| 策略版本 | 945 |
| JSON 策略文档 | 945 |
| 了解更多信息 | 946 |

| | |
|---|-----|
| AmazonSageMakerFullAccess | 947 |
| 使用此策略 | 947 |
| 策略详细信息 | 947 |
| 策略版本 | 947 |
| JSON 策略文档 | 947 |
| 了解更多信息 | 963 |
| AmazonSageMakerGeospatialExecutionRole | 963 |
| 使用此策略 | 963 |
| 策略详细信息 | 963 |
| 策略版本 | 964 |
| JSON 策略文档 | 964 |
| 了解更多信息 | 964 |
| AmazonSageMakerGeospatialFullAccess | 965 |
| 使用此策略 | 965 |
| 策略详细信息 | 965 |
| 策略版本 | 965 |
| JSON 策略文档 | 965 |
| 了解更多信息 | 966 |
| AmazonSageMakerGroundTruthExecution | 966 |
| 使用此策略 | 966 |
| 策略详细信息 | 966 |
| 策略版本 | 967 |
| JSON 策略文档 | 967 |
| 了解更多信息 | 970 |
| AmazonSageMakerMechanicalTurkAccess | 970 |
| 使用此策略 | 971 |
| 策略详细信息 | 971 |
| 策略版本 | 971 |
| JSON 策略文档 | 971 |
| 了解更多信息 | 971 |
| AmazonSageMakerModelGovernanceUseAccess | 972 |
| 使用此策略 | 972 |
| 策略详细信息 | 972 |
| 策略版本 | 972 |
| JSON 策略文档 | 972 |
| 了解更多信息 | 974 |

| | |
|---|-----|
| AmazonSageMakerModelRegistryFullAccess | 974 |
| 使用此策略 | 974 |
| 策略详细信息 | 974 |
| 策略版本 | 975 |
| JSON 策略文档 | 975 |
| 了解更多信息 | 978 |
| AmazonSageMakerNotebooksServiceRolePolicy | 978 |
| 使用此策略 | 978 |
| 策略详细信息 | 978 |
| 策略版本 | 978 |
| JSON 策略文档 | 979 |
| 了解更多信息 | 982 |
| AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy | 982 |
| 使用此策略 | 982 |
| 策略详细信息 | 982 |
| 策略版本 | 982 |
| JSON 策略文档 | 983 |
| 了解更多信息 | 983 |
| AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy | 984 |
| 使用此策略 | 984 |
| 策略详细信息 | 984 |
| 策略版本 | 984 |
| JSON 策略文档 | 984 |
| 了解更多信息 | 988 |
| AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy | 988 |
| 使用此策略 | 988 |
| 策略详细信息 | 988 |
| 策略版本 | 988 |
| JSON 策略文档 | 989 |
| 了解更多信息 | 989 |
| AmazonSageMakerPipelinesIntegrations | 989 |
| 使用此策略 | 990 |
| 策略详细信息 | 990 |
| 策略版本 | 990 |
| JSON 策略文档 | 990 |
| 了解更多信息 | 992 |

| | |
|--|------|
| AmazonSageMakerReadOnly | 992 |
| 使用此策略 | 992 |
| 策略详细信息 | 992 |
| 策略版本 | 992 |
| JSON 策略文档 | 993 |
| 了解更多信息 | 994 |
| AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy | 994 |
| 使用此策略 | 994 |
| 策略详细信息 | 994 |
| 策略版本 | 994 |
| JSON 策略文档 | 995 |
| 了解更多信息 | 995 |
| AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy | 996 |
| 使用此策略 | 996 |
| 策略详细信息 | 996 |
| 策略版本 | 996 |
| JSON 策略文档 | 996 |
| 了解更多信息 | 1003 |
| AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy | 1003 |
| 使用此策略 | 1003 |
| 策略详细信息 | 1003 |
| 策略版本 | 1004 |
| JSON 策略文档 | 1004 |
| 了解更多信息 | 1013 |
| AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy | 1013 |
| 使用此策略 | 1013 |
| 策略详细信息 | 1014 |
| 策略版本 | 1014 |
| JSON 策略文档 | 1014 |
| 了解更多信息 | 1016 |
| AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy | 1016 |
| 使用此策略 | 1016 |
| 策略详细信息 | 1016 |
| 策略版本 | 1016 |
| JSON 策略文档 | 1016 |
| 了解更多信息 | 1017 |

| | |
|--|------|
| AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy | 1017 |
| 使用此策略 | 1017 |
| 策略详细信息 | 1017 |
| 策略版本 | 1018 |
| JSON 策略文档 | 1018 |
| 了解更多信息 | 1018 |
| AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy | 1018 |
| 使用此策略 | 1019 |
| 策略详细信息 | 1019 |
| 策略版本 | 1019 |
| JSON 策略文档 | 1019 |
| 了解更多信息 | 1021 |
| AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy | 1021 |
| 使用此策略 | 1022 |
| 策略详细信息 | 1022 |
| 策略版本 | 1022 |
| JSON 策略文档 | 1022 |
| 了解更多信息 | 1032 |
| AmazonSecurityLakeAdministrator | 1032 |
| 使用此策略 | 1032 |
| 策略详细信息 | 1032 |
| 策略版本 | 1032 |
| JSON 策略文档 | 1032 |
| 了解更多信息 | 1044 |
| AmazonSecurityLakeMetastoreManager | 1044 |
| 使用此策略 | 1044 |
| 策略详细信息 | 1044 |
| 策略版本 | 1044 |
| JSON 策略文档 | 1044 |
| 了解更多信息 | 1046 |
| AmazonSecurityLakePermissionsBoundary | 1047 |
| 使用此策略 | 1047 |
| 策略详细信息 | 1047 |
| 策略版本 | 1047 |
| JSON 策略文档 | 1047 |
| 了解更多信息 | 1050 |

| | |
|-------------------------------|------|
| AmazonSESEFullAccess | 1050 |
| 使用此策略 | 1050 |
| 策略详细信息 | 1051 |
| 策略版本 | 1051 |
| JSON 策略文档 | 1051 |
| 了解更多信息 | 1051 |
| AmazonSESReadOnlyAccess | 1052 |
| 使用此策略 | 1052 |
| 策略详细信息 | 1052 |
| 策略版本 | 1052 |
| JSON 策略文档 | 1052 |
| 了解更多信息 | 1053 |
| AmazonSNSFullAccess | 1053 |
| 使用此策略 | 1053 |
| 策略详细信息 | 1053 |
| 策略版本 | 1053 |
| JSON 策略文档 | 1053 |
| 了解更多信息 | 1054 |
| AmazonSNSReadOnlyAccess | 1054 |
| 使用此策略 | 1054 |
| 策略详细信息 | 1054 |
| 策略版本 | 1054 |
| JSON 策略文档 | 1055 |
| 了解更多信息 | 1055 |
| AmazonSNSRole | 1055 |
| 使用此策略 | 1055 |
| 策略详细信息 | 1055 |
| 策略版本 | 1056 |
| JSON 策略文档 | 1056 |
| 了解更多信息 | 1056 |
| AmazonSQSFullAccess | 1056 |
| 使用此策略 | 1057 |
| 策略详细信息 | 1057 |
| 策略版本 | 1057 |
| JSON 策略文档 | 1057 |
| 了解更多信息 | 1057 |

| | |
|---|------|
| AmazonSQSReadOnlyAccess | 1058 |
| 使用此策略 | 1058 |
| 策略详细信息 | 1058 |
| 策略版本 | 1058 |
| JSON 策略文档 | 1058 |
| 了解更多信息 | 1059 |
| AmazonSSMAutomationApproverAccess | 1059 |
| 使用此策略 | 1059 |
| 策略详细信息 | 1059 |
| 策略版本 | 1059 |
| JSON 策略文档 | 1060 |
| 了解更多信息 | 1060 |
| AmazonSSMAutomationRole | 1060 |
| 使用此策略 | 1060 |
| 策略详细信息 | 1060 |
| 策略版本 | 1061 |
| JSON 策略文档 | 1061 |
| 了解更多信息 | 1062 |
| AmazonSSMDirectoryServiceAccess | 1062 |
| 使用此策略 | 1063 |
| 策略详细信息 | 1063 |
| 策略版本 | 1063 |
| JSON 策略文档 | 1063 |
| 了解更多信息 | 1063 |
| AmazonSSMFullAccess | 1064 |
| 使用此策略 | 1064 |
| 策略详细信息 | 1064 |
| 策略版本 | 1064 |
| JSON 策略文档 | 1064 |
| 了解更多信息 | 1065 |
| AmazonSSMMaintenanceWindowRole | 1066 |
| 使用此策略 | 1066 |
| 策略详细信息 | 1066 |
| 策略版本 | 1066 |
| JSON 策略文档 | 1066 |
| 了解更多信息 | 1068 |

| | |
|--|------|
| AmazonSSMManagedEC2InstanceDefaultPolicy | 1068 |
| 使用此策略 | 1068 |
| 策略详细信息 | 1068 |
| 策略版本 | 1068 |
| JSON 策略文档 | 1068 |
| 了解更多信息 | 1070 |
| AmazonSSMManagedInstanceCore | 1070 |
| 使用此策略 | 1070 |
| 策略详细信息 | 1070 |
| 策略版本 | 1070 |
| JSON 策略文档 | 1070 |
| 了解更多信息 | 1072 |
| AmazonSSMPatchAssociation | 1072 |
| 使用此策略 | 1072 |
| 策略详细信息 | 1072 |
| 策略版本 | 1072 |
| JSON 策略文档 | 1072 |
| 了解更多信息 | 1073 |
| AmazonSSMReadOnlyAccess | 1073 |
| 使用此策略 | 1073 |
| 策略详细信息 | 1073 |
| 策略版本 | 1074 |
| JSON 策略文档 | 1074 |
| 了解更多信息 | 1074 |
| AmazonSSMServiceRolePolicy | 1074 |
| 使用此策略 | 1075 |
| 策略详细信息 | 1075 |
| 策略版本 | 1075 |
| JSON 策略文档 | 1075 |
| 了解更多信息 | 1080 |
| AmazonSumerianFullAccess | 1080 |
| 使用此策略 | 1080 |
| 策略详细信息 | 1080 |
| 策略版本 | 1081 |
| JSON 策略文档 | 1081 |
| 了解更多信息 | 1081 |

| | |
|---|------|
| AmazonTextractFullAccess | 1081 |
| 使用此策略 | 1082 |
| 策略详细信息 | 1082 |
| 策略版本 | 1082 |
| JSON 策略文档 | 1082 |
| 了解更多信息 | 1082 |
| AmazonTextractServiceRole | 1083 |
| 使用此策略 | 1083 |
| 策略详细信息 | 1083 |
| 策略版本 | 1083 |
| JSON 策略文档 | 1083 |
| 了解更多信息 | 1084 |
| AmazonTimestreamConsoleFullAccess | 1084 |
| 使用此策略 | 1084 |
| 策略详细信息 | 1084 |
| 策略版本 | 1084 |
| JSON 策略文档 | 1084 |
| 了解更多信息 | 1086 |
| AmazonTimestreamFullAccess | 1086 |
| 使用此策略 | 1086 |
| 策略详细信息 | 1087 |
| 策略版本 | 1087 |
| JSON 策略文档 | 1087 |
| 了解更多信息 | 1088 |
| AmazonTimestreamInfluxDBFullAccess | 1088 |
| 使用此策略 | 1088 |
| 策略详细信息 | 1088 |
| 策略版本 | 1089 |
| JSON 策略文档 | 1089 |
| 了解更多信息 | 1091 |
| AmazonTimestreamInfluxDBServiceRolePolicy | 1091 |
| 使用此策略 | 1091 |
| 策略详细信息 | 1091 |
| 策略版本 | 1091 |
| JSON 策略文档 | 1092 |
| 了解更多信息 | 1094 |

| | |
|---|------|
| AmazonTimestreamReadOnlyAccess | 1094 |
| 使用此策略 | 1094 |
| 策略详细信息 | 1095 |
| 策略版本 | 1095 |
| JSON 策略文档 | 1095 |
| 了解更多信息 | 1096 |
| AmazonTranscribeFullAccess | 1096 |
| 使用此策略 | 1096 |
| 策略详细信息 | 1096 |
| 策略版本 | 1096 |
| JSON 策略文档 | 1096 |
| 了解更多信息 | 1097 |
| AmazonTranscribeReadOnlyAccess | 1097 |
| 使用此策略 | 1097 |
| 策略详细信息 | 1097 |
| 策略版本 | 1098 |
| JSON 策略文档 | 1098 |
| 了解更多信息 | 1098 |
| AmazonVPCCrossAccountNetworkInterfaceOperations | 1098 |
| 使用此策略 | 1099 |
| 策略详细信息 | 1099 |
| 策略版本 | 1099 |
| JSON 策略文档 | 1099 |
| 了解更多信息 | 1100 |
| AmazonVPCFullAccess | 1101 |
| 使用此策略 | 1101 |
| 策略详细信息 | 1101 |
| 策略版本 | 1101 |
| JSON 策略文档 | 1101 |
| 了解更多信息 | 1105 |
| AmazonVPCNetworkAccessAnalyzerFullAccessPolicy | 1105 |
| 使用此策略 | 1105 |
| 策略详细信息 | 1106 |
| 策略版本 | 1106 |
| JSON 策略文档 | 1106 |
| 了解更多信息 | 1109 |

| | |
|--|------|
| AmazonVPCReachabilityAnalyzerFullAccessPolicy | 1109 |
| 使用此策略 | 1109 |
| 策略详细信息 | 1109 |
| 策略版本 | 1110 |
| JSON 策略文档 | 1110 |
| 了解更多信息 | 1113 |
| AmazonVPCReachabilityAnalyzerPathComponentReadPolicy | 1113 |
| 使用此策略 | 1113 |
| 策略详细信息 | 1113 |
| 策略版本 | 1113 |
| JSON 策略文档 | 1114 |
| 了解更多信息 | 1114 |
| AmazonVPCReadOnlyAccess | 1114 |
| 使用此策略 | 1114 |
| 策略详细信息 | 1114 |
| 策略版本 | 1115 |
| JSON 策略文档 | 1115 |
| 了解更多信息 | 1116 |
| AmazonWorkDocsFullAccess | 1116 |
| 使用此策略 | 1116 |
| 策略详细信息 | 1116 |
| 策略版本 | 1117 |
| JSON 策略文档 | 1117 |
| 了解更多信息 | 1117 |
| AmazonWorkDocsReadOnlyAccess | 1118 |
| 使用此策略 | 1118 |
| 策略详细信息 | 1118 |
| 策略版本 | 1118 |
| JSON 策略文档 | 1118 |
| 了解更多信息 | 1119 |
| AmazonWorkMailEventsServiceRolePolicy | 1119 |
| 使用此策略 | 1119 |
| 策略详细信息 | 1119 |
| 策略版本 | 1119 |
| JSON 策略文档 | 1119 |
| 了解更多信息 | 1120 |

| | |
|---|------|
| AmazonWorkMailFullAccess | 1120 |
| 使用此策略 | 1120 |
| 策略详细信息 | 1120 |
| 策略版本 | 1120 |
| JSON 策略文档 | 1121 |
| 了解更多信息 | 1123 |
| AmazonWorkMailMessageFlowFullAccess | 1123 |
| 使用此策略 | 1123 |
| 策略详细信息 | 1123 |
| 策略版本 | 1123 |
| JSON 策略文档 | 1123 |
| 了解更多信息 | 1124 |
| AmazonWorkMailMessageFlowReadOnlyAccess | 1124 |
| 使用此策略 | 1124 |
| 策略详细信息 | 1124 |
| 策略版本 | 1124 |
| JSON 策略文档 | 1125 |
| 了解更多信息 | 1125 |
| AmazonWorkMailReadOnlyAccess | 1125 |
| 使用此策略 | 1125 |
| 策略详细信息 | 1125 |
| 策略版本 | 1126 |
| JSON 策略文档 | 1126 |
| 了解更多信息 | 1126 |
| AmazonWorkSpacesAdmin | 1127 |
| 使用此策略 | 1127 |
| 策略详细信息 | 1127 |
| 策略版本 | 1127 |
| JSON 策略文档 | 1127 |
| 了解更多信息 | 1128 |
| AmazonWorkSpacesApplicationManagerAdminAccess | 1128 |
| 使用此策略 | 1128 |
| 策略详细信息 | 1128 |
| 策略版本 | 1129 |
| JSON 策略文档 | 1129 |
| 了解更多信息 | 1129 |

| | |
|--|------|
| AmazonWorkspacesPCAAccess | 1129 |
| 使用此策略 | 1130 |
| 策略详细信息 | 1130 |
| 策略版本 | 1130 |
| JSON 策略文档 | 1130 |
| 了解更多信息 | 1131 |
| AmazonWorkSpacesSelfServiceAccess | 1131 |
| 使用此策略 | 1131 |
| 策略详细信息 | 1131 |
| 策略版本 | 1131 |
| JSON 策略文档 | 1131 |
| 了解更多信息 | 1132 |
| AmazonWorkSpacesServiceAccess | 1132 |
| 使用此策略 | 1132 |
| 策略详细信息 | 1132 |
| 策略版本 | 1132 |
| JSON 策略文档 | 1133 |
| 了解更多信息 | 1133 |
| AmazonWorkSpacesWebReadOnly | 1133 |
| 使用此策略 | 1133 |
| 策略详细信息 | 1133 |
| 策略版本 | 1134 |
| JSON 策略文档 | 1134 |
| 了解更多信息 | 1135 |
| AmazonWorkSpacesWebServiceRolePolicy | 1135 |
| 使用此策略 | 1135 |
| 策略详细信息 | 1135 |
| 策略版本 | 1136 |
| JSON 策略文档 | 1136 |
| 了解更多信息 | 1138 |
| AmazonZocaloFullAccess | 1138 |
| 使用此策略 | 1138 |
| 策略详细信息 | 1138 |
| 策略版本 | 1139 |
| JSON 策略文档 | 1139 |
| 了解更多信息 | 1139 |

| | |
|--|------|
| AmazonZocaloReadOnlyAccess | 1140 |
| 使用此策略 | 1140 |
| 策略详细信息 | 1140 |
| 策略版本 | 1140 |
| JSON 策略文档 | 1140 |
| 了解更多信息 | 1141 |
| AmplifyBackendDeployFullAccess | 1141 |
| 使用此策略 | 1141 |
| 策略详细信息 | 1141 |
| 策略版本 | 1141 |
| JSON 策略文档 | 1142 |
| 了解更多信息 | 1145 |
| APIGatewayServiceRolePolicy | 1145 |
| 使用此策略 | 1145 |
| 策略详细信息 | 1145 |
| 策略版本 | 1145 |
| JSON 策略文档 | 1145 |
| 了解更多信息 | 1148 |
| AppIntegrationsServiceLinkedRolePolicy | 1148 |
| 使用此策略 | 1148 |
| 策略详细信息 | 1148 |
| 策略版本 | 1148 |
| JSON 策略文档 | 1148 |
| 了解更多信息 | 1150 |
| ApplicationAutoScalingForAmazonAppStreamAccess | 1150 |
| 使用此策略 | 1150 |
| 策略详细信息 | 1150 |
| 策略版本 | 1151 |
| JSON 策略文档 | 1151 |
| 了解更多信息 | 1151 |
| ApplicationDiscoveryServiceContinuousExportServiceRolePolicy | 1152 |
| 使用此策略 | 1152 |
| 策略详细信息 | 1152 |
| 策略版本 | 1152 |
| JSON 策略文档 | 1152 |
| 了解更多信息 | 1154 |

| | |
|--|------|
| AppRunnerNetworkingServiceRolePolicy | 1154 |
| 使用此策略 | 1154 |
| 策略详细信息 | 1155 |
| 策略版本 | 1155 |
| JSON 策略文档 | 1155 |
| 了解更多信息 | 1156 |
| AppRunnerServiceRolePolicy | 1156 |
| 使用此策略 | 1157 |
| 策略详细信息 | 1157 |
| 策略版本 | 1157 |
| JSON 策略文档 | 1157 |
| 了解更多信息 | 1158 |
| AutoScalingConsoleFullAccess | 1158 |
| 使用此策略 | 1158 |
| 策略详细信息 | 1158 |
| 策略版本 | 1159 |
| JSON 策略文档 | 1159 |
| 了解更多信息 | 1160 |
| AutoScalingConsoleReadOnlyAccess | 1161 |
| 使用此策略 | 1161 |
| 策略详细信息 | 1161 |
| 策略版本 | 1161 |
| JSON 策略文档 | 1161 |
| 了解更多信息 | 1162 |
| AutoScalingFullAccess | 1163 |
| 使用此策略 | 1163 |
| 策略详细信息 | 1163 |
| 策略版本 | 1163 |
| JSON 策略文档 | 1163 |
| 了解更多信息 | 1164 |
| AutoScalingNotificationAccessRole | 1165 |
| 使用此策略 | 1165 |
| 策略详细信息 | 1165 |
| 策略版本 | 1165 |
| JSON 策略文档 | 1165 |
| 了解更多信息 | 1166 |

| | |
|--|------|
| AutoScalingReadOnlyAccess | 1166 |
| 使用此策略 | 1166 |
| 策略详细信息 | 1166 |
| 策略版本 | 1166 |
| JSON 策略文档 | 1166 |
| 了解更多信息 | 1167 |
| AutoScalingServiceRolePolicy | 1167 |
| 使用此策略 | 1167 |
| 策略详细信息 | 1167 |
| 策略版本 | 1167 |
| JSON 策略文档 | 1168 |
| 了解更多信息 | 1170 |
| AWS_ConfigRole | 1171 |
| 使用此策略 | 1171 |
| 策略详细信息 | 1171 |
| 策略版本 | 1171 |
| JSON 策略文档 | 1171 |
| 了解更多信息 | 1202 |
| AWSAccountActivityAccess | 1202 |
| 使用此策略 | 1202 |
| 策略详细信息 | 1202 |
| 策略版本 | 1202 |
| JSON 策略文档 | 1203 |
| 了解更多信息 | 1203 |
| AWSAccountManagementFullAccess | 1204 |
| 使用此策略 | 1204 |
| 策略详细信息 | 1204 |
| 策略版本 | 1204 |
| JSON 策略文档 | 1204 |
| 了解更多信息 | 1204 |
| AWSAccountManagementReadOnlyAccess | 1205 |
| 使用此策略 | 1205 |
| 策略详细信息 | 1205 |
| 策略版本 | 1205 |
| JSON 策略文档 | 1205 |
| 了解更多信息 | 1206 |

| | |
|---|------|
| AWSAccountUsageReportAccess | 1206 |
| 使用此策略 | 1206 |
| 策略详细信息 | 1206 |
| 策略版本 | 1206 |
| JSON 策略文档 | 1206 |
| 了解更多信息 | 1207 |
| AWSAgentlessDiscoveryService | 1207 |
| 使用此策略 | 1207 |
| 策略详细信息 | 1207 |
| 策略版本 | 1207 |
| JSON 策略文档 | 1208 |
| 了解更多信息 | 1209 |
| AWSAppFabricFullAccess | 1210 |
| 使用此策略 | 1210 |
| 策略详细信息 | 1210 |
| 策略版本 | 1210 |
| JSON 策略文档 | 1210 |
| 了解更多信息 | 1212 |
| AWSAppFabricReadOnlyAccess | 1212 |
| 使用此策略 | 1212 |
| 策略详细信息 | 1212 |
| 策略版本 | 1212 |
| JSON 策略文档 | 1212 |
| 了解更多信息 | 1213 |
| AWSAppFabricServiceRolePolicy | 1213 |
| 使用此策略 | 1213 |
| 策略详细信息 | 1213 |
| 策略版本 | 1214 |
| JSON 策略文档 | 1214 |
| 了解更多信息 | 1215 |
| AWSApplicationAutoscalingAppStreamFleetPolicy | 1215 |
| 使用此策略 | 1215 |
| 策略详细信息 | 1215 |
| 策略版本 | 1215 |
| JSON 策略文档 | 1216 |
| 了解更多信息 | 1216 |

| | |
|--|------|
| AWSApplicationAutoscalingCassandraTablePolicy | 1216 |
| 使用此策略 | 1216 |
| 策略详细信息 | 1217 |
| 策略版本 | 1217 |
| JSON 策略文档 | 1217 |
| 了解更多信息 | 1218 |
| AWSApplicationAutoscalingComprehendEndpointPolicy | 1218 |
| 使用此策略 | 1218 |
| 策略详细信息 | 1218 |
| 策略版本 | 1218 |
| JSON 策略文档 | 1218 |
| 了解更多信息 | 1219 |
| AWSApplicationAutoScalingCustomResourcePolicy | 1219 |
| 使用此策略 | 1219 |
| 策略详细信息 | 1219 |
| 策略版本 | 1220 |
| JSON 策略文档 | 1220 |
| 了解更多信息 | 1220 |
| AWSApplicationAutoscalingDynamoDBTablePolicy | 1220 |
| 使用此策略 | 1220 |
| 策略详细信息 | 1221 |
| 策略版本 | 1221 |
| JSON 策略文档 | 1221 |
| 了解更多信息 | 1221 |
| AWSApplicationAutoscalingEC2SpotFleetRequestPolicy | 1222 |
| 使用此策略 | 1222 |
| 策略详细信息 | 1222 |
| 策略版本 | 1222 |
| JSON 策略文档 | 1222 |
| 了解更多信息 | 1223 |
| AWSApplicationAutoscalingECSServicePolicy | 1223 |
| 使用此策略 | 1223 |
| 策略详细信息 | 1223 |
| 策略版本 | 1223 |
| JSON 策略文档 | 1223 |
| 了解更多信息 | 1224 |

| | |
|--|------|
| AWSApplicationAutoscalingElastiCacheRGPolicy | 1224 |
| 使用此策略 | 1224 |
| 策略详细信息 | 1224 |
| 策略版本 | 1225 |
| JSON 策略文档 | 1225 |
| 了解更多信息 | 1226 |
| AWSApplicationAutoscalingEMRInstanceGroupPolicy | 1226 |
| 使用此策略 | 1226 |
| 策略详细信息 | 1226 |
| 策略版本 | 1226 |
| JSON 策略文档 | 1226 |
| 了解更多信息 | 1227 |
| AWSApplicationAutoscalingKafkaClusterPolicy | 1227 |
| 使用此策略 | 1227 |
| 策略详细信息 | 1227 |
| 策略版本 | 1227 |
| JSON 策略文档 | 1228 |
| 了解更多信息 | 1228 |
| AWSApplicationAutoscalingLambdaConcurrencyPolicy | 1228 |
| 使用此策略 | 1228 |
| 策略详细信息 | 1228 |
| 策略版本 | 1229 |
| JSON 策略文档 | 1229 |
| 了解更多信息 | 1229 |
| AWSApplicationAutoscalingNeptuneClusterPolicy | 1230 |
| 使用此策略 | 1230 |
| 策略详细信息 | 1230 |
| 策略版本 | 1230 |
| JSON 策略文档 | 1230 |
| 了解更多信息 | 1232 |
| AWSApplicationAutoscalingRDSClusterPolicy | 1232 |
| 使用此策略 | 1232 |
| 策略详细信息 | 1232 |
| 策略版本 | 1232 |
| JSON 策略文档 | 1232 |
| 了解更多信息 | 1233 |

| | |
|--|------|
| AWSApplicationAutoscalingSageMakerEndpointPolicy | 1233 |
| 使用此策略 | 1234 |
| 策略详细信息 | 1234 |
| 策略版本 | 1234 |
| JSON 策略文档 | 1234 |
| 了解更多信息 | 1235 |
| AWSApplicationDiscoveryAgentAccess | 1235 |
| 使用此策略 | 1235 |
| 策略详细信息 | 1235 |
| 策略版本 | 1235 |
| JSON 策略文档 | 1236 |
| 了解更多信息 | 1236 |
| AWSApplicationDiscoveryAgentlessCollectorAccess | 1236 |
| 使用此策略 | 1237 |
| 策略详细信息 | 1237 |
| 策略版本 | 1237 |
| JSON 策略文档 | 1237 |
| 了解更多信息 | 1238 |
| AWSApplicationDiscoveryServiceFullAccess | 1238 |
| 使用此策略 | 1238 |
| 策略详细信息 | 1239 |
| 策略版本 | 1239 |
| JSON 策略文档 | 1239 |
| 了解更多信息 | 1240 |
| AWSApplicationMigrationAgentInstallationPolicy | 1241 |
| 使用此策略 | 1241 |
| 策略详细信息 | 1241 |
| 策略版本 | 1241 |
| JSON 策略文档 | 1241 |
| 了解更多信息 | 1242 |
| AWSApplicationMigrationAgentPolicy | 1242 |
| 使用此策略 | 1242 |
| 策略详细信息 | 1243 |
| 策略版本 | 1243 |
| JSON 策略文档 | 1243 |
| 了解更多信息 | 1244 |

| | |
|---|------|
| AWSApplicationMigrationAgentPolicy_v2 | 1244 |
| 使用此策略 | 1244 |
| 策略详细信息 | 1244 |
| 策略版本 | 1245 |
| JSON 策略文档 | 1245 |
| 了解更多信息 | 1245 |
| AWSApplicationMigrationConversionServerPolicy | 1246 |
| 使用此策略 | 1246 |
| 策略详细信息 | 1246 |
| 策略版本 | 1246 |
| JSON 策略文档 | 1246 |
| 了解更多信息 | 1247 |
| AWSApplicationMigrationEC2Access | 1247 |
| 使用此策略 | 1247 |
| 策略详细信息 | 1247 |
| 策略版本 | 1247 |
| JSON 策略文档 | 1248 |
| 了解更多信息 | 1255 |
| AWSApplicationMigrationFullAccess | 1256 |
| 使用此策略 | 1256 |
| 策略详细信息 | 1256 |
| 策略版本 | 1256 |
| JSON 策略文档 | 1256 |
| 了解更多信息 | 1261 |
| AWSApplicationMigrationMGHAccess | 1262 |
| 使用此策略 | 1262 |
| 策略详细信息 | 1262 |
| 策略版本 | 1262 |
| JSON 策略文档 | 1262 |
| 了解更多信息 | 1263 |
| AWSApplicationMigrationReadOnlyAccess | 1263 |
| 使用此策略 | 1263 |
| 策略详细信息 | 1263 |
| 策略版本 | 1263 |
| JSON 策略文档 | 1264 |
| 了解更多信息 | 1265 |

| | |
|---|------|
| AWSApplicationMigrationReplicationServerPolicy | 1265 |
| 使用此策略 | 1265 |
| 策略详细信息 | 1265 |
| 策略版本 | 1266 |
| JSON 策略文档 | 1266 |
| 了解更多信息 | 1267 |
| AWSApplicationMigrationServiceEc2InstancePolicy | 1268 |
| 使用此策略 | 1268 |
| 策略详细信息 | 1268 |
| 策略版本 | 1268 |
| JSON 策略文档 | 1268 |
| 了解更多信息 | 1269 |
| AWSApplicationMigrationServiceRolePolicy | 1270 |
| 使用此策略 | 1270 |
| 策略详细信息 | 1270 |
| 策略版本 | 1270 |
| JSON 策略文档 | 1270 |
| 了解更多信息 | 1277 |
| AWSApplicationMigrationSSMAccess | 1277 |
| 使用此策略 | 1278 |
| 策略详细信息 | 1278 |
| 策略版本 | 1278 |
| JSON 策略文档 | 1278 |
| 了解更多信息 | 1280 |
| AWSApplicationMigrationVCenterClientPolicy | 1280 |
| 使用此策略 | 1280 |
| 策略详细信息 | 1280 |
| 策略版本 | 1281 |
| JSON 策略文档 | 1281 |
| 了解更多信息 | 1281 |
| AWSAppMeshEnvoyAccess | 1282 |
| 使用此策略 | 1282 |
| 策略详细信息 | 1282 |
| 策略版本 | 1282 |
| JSON 策略文档 | 1282 |
| 了解更多信息 | 1283 |

| | |
|--|------|
| AWSAppMeshFullAccess | 1283 |
| 使用此策略 | 1283 |
| 策略详细信息 | 1283 |
| 策略版本 | 1283 |
| JSON 策略文档 | 1283 |
| 了解更多信息 | 1285 |
| AWSAppMeshPreviewEnvoyAccess | 1285 |
| 使用此策略 | 1285 |
| 策略详细信息 | 1285 |
| 策略版本 | 1285 |
| JSON 策略文档 | 1286 |
| 了解更多信息 | 1286 |
| AWSAppMeshPreviewServiceRolePolicy | 1286 |
| 使用此策略 | 1286 |
| 策略详细信息 | 1286 |
| 策略版本 | 1287 |
| JSON 策略文档 | 1287 |
| 了解更多信息 | 1287 |
| AWSAppMeshReadOnly | 1287 |
| 使用此策略 | 1288 |
| 策略详细信息 | 1288 |
| 策略版本 | 1288 |
| JSON 策略文档 | 1288 |
| 了解更多信息 | 1289 |
| AWSAppMeshServiceRolePolicy | 1289 |
| 使用此策略 | 1289 |
| 策略详细信息 | 1289 |
| 策略版本 | 1290 |
| JSON 策略文档 | 1290 |
| 了解更多信息 | 1290 |
| AWSAppRunnerFullAccess | 1291 |
| 使用此策略 | 1291 |
| 策略详细信息 | 1291 |
| 策略版本 | 1291 |
| JSON 策略文档 | 1291 |
| 了解更多信息 | 1292 |

| | |
|---|------|
| AWSAppRunnerReadOnlyAccess | 1292 |
| 使用此策略 | 1292 |
| 策略详细信息 | 1292 |
| 策略版本 | 1293 |
| JSON 策略文档 | 1293 |
| 了解更多信息 | 1293 |
| AWSAppRunnerServicePolicyForECRAccess | 1293 |
| 使用此策略 | 1293 |
| 策略详细信息 | 1294 |
| 策略版本 | 1294 |
| JSON 策略文档 | 1294 |
| 了解更多信息 | 1294 |
| AWSAppSyncAdministrator | 1295 |
| 使用此策略 | 1295 |
| 策略详细信息 | 1295 |
| 策略版本 | 1295 |
| JSON 策略文档 | 1295 |
| 了解更多信息 | 1296 |
| AWSAppSyncInvokeFullAccess | 1297 |
| 使用此策略 | 1297 |
| 策略详细信息 | 1297 |
| 策略版本 | 1297 |
| JSON 策略文档 | 1297 |
| 了解更多信息 | 1298 |
| AWSAppSyncPushToCloudWatchLogs | 1298 |
| 使用此策略 | 1298 |
| 策略详细信息 | 1298 |
| 策略版本 | 1298 |
| JSON 策略文档 | 1298 |
| 了解更多信息 | 1299 |
| AWSAppSyncSchemaAuthor | 1299 |
| 使用此策略 | 1299 |
| 策略详细信息 | 1299 |
| 策略版本 | 1299 |
| JSON 策略文档 | 1300 |
| 了解更多信息 | 1301 |

| | |
|--|------|
| AWSAppSyncServiceRolePolicy | 1301 |
| 使用此策略 | 1301 |
| 策略详细信息 | 1301 |
| 策略版本 | 1301 |
| JSON 策略文档 | 1301 |
| 了解更多信息 | 1302 |
| AWSArtifactAccountSync | 1302 |
| 使用此策略 | 1302 |
| 策略详细信息 | 1302 |
| 策略版本 | 1303 |
| JSON 策略文档 | 1303 |
| 了解更多信息 | 1303 |
| AWSArtifactReportsReadOnlyAccess | 1303 |
| 使用此策略 | 1303 |
| 策略详细信息 | 1304 |
| 策略版本 | 1304 |
| JSON 策略文档 | 1304 |
| 了解更多信息 | 1304 |
| AWSArtifactServiceRolePolicy | 1305 |
| 使用此策略 | 1305 |
| 策略详细信息 | 1305 |
| 策略版本 | 1305 |
| JSON 策略文档 | 1305 |
| 了解更多信息 | 1306 |
| AWSAuditManagerAdministratorAccess | 1306 |
| 使用此策略 | 1306 |
| 策略详细信息 | 1306 |
| 策略版本 | 1306 |
| JSON 策略文档 | 1306 |
| 了解更多信息 | 1310 |
| AWSAuditManagerServiceRolePolicy | 1310 |
| 使用此策略 | 1310 |
| 策略详细信息 | 1311 |
| 策略版本 | 1311 |
| JSON 策略文档 | 1311 |
| 了解更多信息 | 1315 |

| | |
|--|------|
| AWSAutoScalingPlansEC2AutoScalingPolicy | 1316 |
| 使用此策略 | 1316 |
| 策略详细信息 | 1316 |
| 策略版本 | 1316 |
| JSON 策略文档 | 1316 |
| 了解更多信息 | 1317 |
| AWSBackupAuditAccess | 1317 |
| 使用此策略 | 1317 |
| 策略详细信息 | 1317 |
| 策略版本 | 1317 |
| JSON 策略文档 | 1317 |
| 了解更多信息 | 1319 |
| AWSBackupDataTransferAccess | 1319 |
| 使用此策略 | 1319 |
| 策略详细信息 | 1319 |
| 策略版本 | 1319 |
| JSON 策略文档 | 1320 |
| 了解更多信息 | 1320 |
| AWSBackupFullAccess | 1320 |
| 使用此策略 | 1320 |
| 策略详细信息 | 1321 |
| 策略版本 | 1321 |
| JSON 策略文档 | 1321 |
| 了解更多信息 | 1331 |
| AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync | 1331 |
| 使用此策略 | 1331 |
| 策略详细信息 | 1331 |
| 策略版本 | 1331 |
| JSON 策略文档 | 1332 |
| 了解更多信息 | 1332 |
| AWSBackupOperatorAccess | 1332 |
| 使用此策略 | 1333 |
| 策略详细信息 | 1333 |
| 策略版本 | 1333 |
| JSON 策略文档 | 1333 |
| 了解更多信息 | 1340 |

| | |
|---|------|
| AWSBackupOrganizationAdminAccess | 1340 |
| 使用此策略 | 1340 |
| 策略详细信息 | 1340 |
| 策略版本 | 1340 |
| JSON 策略文档 | 1341 |
| 了解更多信息 | 1342 |
| AWSBackupRestoreAccessForSAPHANA | 1343 |
| 使用此策略 | 1343 |
| 策略详细信息 | 1343 |
| 策略版本 | 1343 |
| JSON 策略文档 | 1343 |
| 了解更多信息 | 1344 |
| AWSBackupServiceLinkedRolePolicyForBackup | 1344 |
| 使用此策略 | 1344 |
| 策略详细信息 | 1345 |
| 策略版本 | 1345 |
| JSON 策略文档 | 1345 |
| 了解更多信息 | 1353 |
| AWSBackupServiceLinkedRolePolicyForBackupTest | 1353 |
| 使用此策略 | 1353 |
| 策略详细信息 | 1353 |
| 策略版本 | 1353 |
| JSON 策略文档 | 1353 |
| 了解更多信息 | 1354 |
| AWSBackupServiceRolePolicyForBackup | 1354 |
| 使用此策略 | 1354 |
| 策略详细信息 | 1354 |
| 策略版本 | 1355 |
| JSON 策略文档 | 1355 |
| 了解更多信息 | 1365 |
| AWSBackupServiceRolePolicyForRestores | 1366 |
| 使用此策略 | 1366 |
| 策略详细信息 | 1366 |
| 策略版本 | 1366 |
| JSON 策略文档 | 1366 |
| 了解更多信息 | 1376 |

| | |
|--|------|
| AWSBackupServiceRolePolicyForS3Backup | 1376 |
| 使用此策略 | 1376 |
| 策略详细信息 | 1377 |
| 策略版本 | 1377 |
| JSON 策略文档 | 1377 |
| 了解更多信息 | 1379 |
| AWSBackupServiceRolePolicyForS3Restore | 1379 |
| 使用此策略 | 1379 |
| 策略详细信息 | 1379 |
| 策略版本 | 1379 |
| JSON 策略文档 | 1380 |
| 了解更多信息 | 1381 |
| AWSBatchFullAccess | 1381 |
| 使用此策略 | 1381 |
| 策略详细信息 | 1381 |
| 策略版本 | 1382 |
| JSON 策略文档 | 1382 |
| 了解更多信息 | 1383 |
| AWSBatchServiceEventTargetRole | 1383 |
| 使用此策略 | 1383 |
| 策略详细信息 | 1384 |
| 策略版本 | 1384 |
| JSON 策略文档 | 1384 |
| 了解更多信息 | 1384 |
| AWSBatchServiceRole | 1385 |
| 使用此策略 | 1385 |
| 策略详细信息 | 1385 |
| 策略版本 | 1385 |
| JSON 策略文档 | 1385 |
| 了解更多信息 | 1388 |
| AWSBillingConductorFullAccess | 1389 |
| 使用此策略 | 1389 |
| 策略详细信息 | 1389 |
| 策略版本 | 1389 |
| JSON 策略文档 | 1389 |
| 了解更多信息 | 1390 |

| | |
|--|------|
| AWSBillingConductorReadOnlyAccess | 1390 |
| 使用此策略 | 1390 |
| 策略详细信息 | 1390 |
| 策略版本 | 1390 |
| JSON 策略文档 | 1390 |
| 了解更多信息 | 1391 |
| AWSBillingReadOnlyAccess | 1391 |
| 使用此策略 | 1391 |
| 策略详细信息 | 1391 |
| 策略版本 | 1392 |
| JSON 策略文档 | 1392 |
| 了解更多信息 | 1393 |
| AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM | 1393 |
| 使用此策略 | 1393 |
| 策略详细信息 | 1394 |
| 策略版本 | 1394 |
| JSON 策略文档 | 1394 |
| 了解更多信息 | 1395 |
| AWSBudgetsActionsWithAWSResourceControlAccess | 1395 |
| 使用此策略 | 1395 |
| 策略详细信息 | 1395 |
| 策略版本 | 1396 |
| JSON 策略文档 | 1396 |
| 了解更多信息 | 1397 |
| AWSBudgetsReadOnlyAccess | 1397 |
| 使用此策略 | 1397 |
| 策略详细信息 | 1397 |
| 策略版本 | 1398 |
| JSON 策略文档 | 1398 |
| 了解更多信息 | 1398 |
| AWSBugBustFullAccess | 1398 |
| 使用此策略 | 1398 |
| 策略详细信息 | 1399 |
| 策略版本 | 1399 |
| JSON 策略文档 | 1399 |
| 了解更多信息 | 1400 |

| | |
|--|------|
| AWSBugBustPlayerAccess | 1400 |
| 使用此策略 | 1400 |
| 策略详细信息 | 1400 |
| 策略版本 | 1401 |
| JSON 策略文档 | 1401 |
| 了解更多信息 | 1402 |
| AWSBugBustServiceRolePolicy | 1402 |
| 使用此策略 | 1402 |
| 策略详细信息 | 1402 |
| 策略版本 | 1402 |
| JSON 策略文档 | 1403 |
| 了解更多信息 | 1403 |
| AWSCertificateManagerFullAccess | 1403 |
| 使用此策略 | 1403 |
| 策略详细信息 | 1404 |
| 策略版本 | 1404 |
| JSON 策略文档 | 1404 |
| 了解更多信息 | 1405 |
| AWSCertificateManagerPrivateCAAuditor | 1405 |
| 使用此策略 | 1405 |
| 策略详细信息 | 1405 |
| 策略版本 | 1405 |
| JSON 策略文档 | 1406 |
| 了解更多信息 | 1406 |
| AWSCertificateManagerPrivateCAFullAccess | 1407 |
| 使用此策略 | 1407 |
| 策略详细信息 | 1407 |
| 策略版本 | 1407 |
| JSON 策略文档 | 1407 |
| 了解更多信息 | 1408 |
| AWSCertificateManagerPrivateCAPrivilegedUser | 1408 |
| 使用此策略 | 1408 |
| 策略详细信息 | 1408 |
| 策略版本 | 1408 |
| JSON 策略文档 | 1408 |
| 了解更多信息 | 1410 |

| | |
|--|------|
| AWSCertificateManagerPrivateCAReadOnly | 1410 |
| 使用此策略 | 1410 |
| 策略详细信息 | 1410 |
| 策略版本 | 1410 |
| JSON 策略文档 | 1410 |
| 了解更多信息 | 1411 |
| AWSCertificateManagerPrivateCAUser | 1411 |
| 使用此策略 | 1411 |
| 策略详细信息 | 1411 |
| 策略版本 | 1412 |
| JSON 策略文档 | 1412 |
| 了解更多信息 | 1413 |
| AWSCertificateManagerReadOnly | 1413 |
| 使用此策略 | 1413 |
| 策略详细信息 | 1413 |
| 策略版本 | 1414 |
| JSON 策略文档 | 1414 |
| 了解更多信息 | 1414 |
| AWSChatbotServiceLinkedRolePolicy | 1414 |
| 使用此策略 | 1415 |
| 策略详细信息 | 1415 |
| 策略版本 | 1415 |
| JSON 策略文档 | 1415 |
| 了解更多信息 | 1416 |
| AWSCleanRoomsFullAccess | 1416 |
| 使用此策略 | 1416 |
| 策略详细信息 | 1416 |
| 策略版本 | 1416 |
| JSON 策略文档 | 1417 |
| 了解更多信息 | 1421 |
| AWSCleanRoomsFullAccessNoQuerying | 1421 |
| 使用此策略 | 1421 |
| 策略详细信息 | 1421 |
| 策略版本 | 1422 |
| JSON 策略文档 | 1422 |
| 了解更多信息 | 1426 |

| | |
|-------------------------------------|------|
| AWSCleanRoomsMLFullAccess | 1427 |
| 使用此策略 | 1427 |
| 策略详细信息 | 1427 |
| 策略版本 | 1427 |
| JSON 策略文档 | 1427 |
| 了解更多信息 | 1431 |
| AWSCleanRoomsMLReadOnlyAccess | 1431 |
| 使用此策略 | 1431 |
| 策略详细信息 | 1431 |
| 策略版本 | 1431 |
| JSON 策略文档 | 1432 |
| 了解更多信息 | 1432 |
| AWSCleanRoomsReadOnlyAccess | 1433 |
| 使用此策略 | 1433 |
| 策略详细信息 | 1433 |
| 策略版本 | 1433 |
| JSON 策略文档 | 1433 |
| 了解更多信息 | 1434 |
| AWSCloud9Administrator | 1435 |
| 使用此策略 | 1435 |
| 策略详细信息 | 1435 |
| 策略版本 | 1435 |
| JSON 策略文档 | 1435 |
| 了解更多信息 | 1437 |
| AWSCloud9EnvironmentMember | 1437 |
| 使用此策略 | 1437 |
| 策略详细信息 | 1437 |
| 策略版本 | 1437 |
| JSON 策略文档 | 1437 |
| 了解更多信息 | 1439 |
| AWSCloud9ServiceRolePolicy | 1439 |
| 使用此策略 | 1439 |
| 策略详细信息 | 1439 |
| 策略版本 | 1439 |
| JSON 策略文档 | 1440 |
| 了解更多信息 | 1442 |

| | |
|---------------------------------------|------|
| AWSCloud9SSMInstanceProfile | 1442 |
| 使用此策略 | 1442 |
| 策略详细信息 | 1442 |
| 策略版本 | 1443 |
| JSON 策略文档 | 1443 |
| 了解更多信息 | 1443 |
| AWSCloud9User | 1443 |
| 使用此策略 | 1443 |
| 策略详细信息 | 1444 |
| 策略版本 | 1444 |
| JSON 策略文档 | 1444 |
| 了解更多信息 | 1446 |
| AWSCloudFormationFullAccess | 1446 |
| 使用此策略 | 1447 |
| 策略详细信息 | 1447 |
| 策略版本 | 1447 |
| JSON 策略文档 | 1447 |
| 了解更多信息 | 1447 |
| AWSCloudFormationReadOnlyAccess | 1448 |
| 使用此策略 | 1448 |
| 策略详细信息 | 1448 |
| 策略版本 | 1448 |
| JSON 策略文档 | 1448 |
| 了解更多信息 | 1449 |
| AWSCloudFrontLogger | 1449 |
| 使用此策略 | 1449 |
| 策略详细信息 | 1449 |
| 策略版本 | 1449 |
| JSON 策略文档 | 1450 |
| 了解更多信息 | 1450 |
| AWSCloudHSMFullAccess | 1450 |
| 使用此策略 | 1450 |
| 策略详细信息 | 1450 |
| 策略版本 | 1451 |
| JSON 策略文档 | 1451 |
| 了解更多信息 | 1451 |

| | |
|---|------|
| AWSCloudHSMReadOnlyAccess | 1451 |
| 使用此策略 | 1451 |
| 策略详细信息 | 1451 |
| 策略版本 | 1452 |
| JSON 策略文档 | 1452 |
| 了解更多信息 | 1452 |
| AWSCloudHSMRole | 1452 |
| 使用此策略 | 1453 |
| 策略详细信息 | 1453 |
| 策略版本 | 1453 |
| JSON 策略文档 | 1453 |
| 了解更多信息 | 1454 |
| AWSCloudMapDiscoverInstanceAccess | 1454 |
| 使用此策略 | 1454 |
| 策略详细信息 | 1454 |
| 策略版本 | 1454 |
| JSON 策略文档 | 1454 |
| 了解更多信息 | 1455 |
| AWSCloudMapFullAccess | 1455 |
| 使用此策略 | 1455 |
| 策略详细信息 | 1455 |
| 策略版本 | 1456 |
| JSON 策略文档 | 1456 |
| 了解更多信息 | 1456 |
| AWSCloudMapReadOnlyAccess | 1457 |
| 使用此策略 | 1457 |
| 策略详细信息 | 1457 |
| 策略版本 | 1457 |
| JSON 策略文档 | 1457 |
| 了解更多信息 | 1458 |
| AWSCloudMapRegisterInstanceAccess | 1458 |
| 使用此策略 | 1458 |
| 策略详细信息 | 1458 |
| 策略版本 | 1458 |
| JSON 策略文档 | 1459 |
| 了解更多信息 | 1459 |

| | |
|---|------|
| AWSCloudShellFullAccess | 1459 |
| 使用此策略 | 1460 |
| 策略详细信息 | 1460 |
| 策略版本 | 1460 |
| JSON 策略文档 | 1460 |
| 了解更多信息 | 1460 |
| AWSCloudTrail_FullAccess | 1461 |
| 使用此策略 | 1461 |
| 策略详细信息 | 1461 |
| 策略版本 | 1461 |
| JSON 策略文档 | 1461 |
| 了解更多信息 | 1464 |
| AWSCloudTrail_ReadOnlyAccess | 1464 |
| 使用此策略 | 1464 |
| 策略详细信息 | 1464 |
| 策略版本 | 1464 |
| JSON 策略文档 | 1464 |
| 了解更多信息 | 1465 |
| AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy | 1465 |
| 使用此策略 | 1465 |
| 策略详细信息 | 1465 |
| 策略版本 | 1466 |
| JSON 策略文档 | 1466 |
| 了解更多信息 | 1466 |
| AWSCodeArtifactAdminAccess | 1466 |
| 使用此策略 | 1466 |
| 策略详细信息 | 1467 |
| 策略版本 | 1467 |
| JSON 策略文档 | 1467 |
| 了解更多信息 | 1468 |
| AWSCodeArtifactReadOnlyAccess | 1468 |
| 使用此策略 | 1468 |
| 策略详细信息 | 1468 |
| 策略版本 | 1468 |
| JSON 策略文档 | 1468 |
| 了解更多信息 | 1469 |

| | |
|-----------------------------------|------|
| AWSCodeBuildAdminAccess | 1469 |
| 使用此策略 | 1469 |
| 策略详细信息 | 1470 |
| 策略版本 | 1470 |
| JSON 策略文档 | 1470 |
| 了解更多信息 | 1473 |
| AWSCodeBuildDeveloperAccess | 1473 |
| 使用此策略 | 1474 |
| 策略详细信息 | 1474 |
| 策略版本 | 1474 |
| JSON 策略文档 | 1474 |
| 了解更多信息 | 1477 |
| AWSCodeBuildReadOnlyAccess | 1477 |
| 使用此策略 | 1477 |
| 策略详细信息 | 1477 |
| 策略版本 | 1477 |
| JSON 策略文档 | 1477 |
| 了解更多信息 | 1479 |
| AWSCodeCommitFullAccess | 1479 |
| 使用此策略 | 1479 |
| 策略详细信息 | 1479 |
| 策略版本 | 1479 |
| JSON 策略文档 | 1480 |
| 了解更多信息 | 1484 |
| AWSCodeCommitPowerUser | 1484 |
| 使用此策略 | 1484 |
| 策略详细信息 | 1485 |
| 策略版本 | 1485 |
| JSON 策略文档 | 1485 |
| 了解更多信息 | 1490 |
| AWSCodeCommitReadOnly | 1490 |
| 使用此策略 | 1490 |
| 策略详细信息 | 1490 |
| 策略版本 | 1490 |
| JSON 策略文档 | 1490 |
| 了解更多信息 | 1493 |

| | |
|--|------|
| AWSCodeDeployDeployerAccess | 1493 |
| 使用此策略 | 1493 |
| 策略详细信息 | 1493 |
| 策略版本 | 1494 |
| JSON 策略文档 | 1494 |
| 了解更多信息 | 1495 |
| AWSCodeDeployFullAccess | 1495 |
| 使用此策略 | 1496 |
| 策略详细信息 | 1496 |
| 策略版本 | 1496 |
| JSON 策略文档 | 1496 |
| 了解更多信息 | 1498 |
| AWSCodeDeployReadOnlyAccess | 1498 |
| 使用此策略 | 1498 |
| 策略详细信息 | 1498 |
| 策略版本 | 1498 |
| JSON 策略文档 | 1498 |
| 了解更多信息 | 1499 |
| AWSCodeDeployRole | 1500 |
| 使用此策略 | 1500 |
| 策略详细信息 | 1500 |
| 策略版本 | 1500 |
| JSON 策略文档 | 1500 |
| 了解更多信息 | 1501 |
| AWSCodeDeployRoleForCloudFormation | 1502 |
| 使用此策略 | 1502 |
| 策略详细信息 | 1502 |
| 策略版本 | 1502 |
| JSON 策略文档 | 1502 |
| 了解更多信息 | 1503 |
| AWSCodeDeployRoleForECS | 1503 |
| 使用此策略 | 1503 |
| 策略详细信息 | 1503 |
| 策略版本 | 1503 |
| JSON 策略文档 | 1504 |
| 了解更多信息 | 1505 |

| | |
|---|------|
| AWSCodeDeployRoleForECSLimited | 1505 |
| 使用此策略 | 1505 |
| 策略详细信息 | 1505 |
| 策略版本 | 1505 |
| JSON 策略文档 | 1505 |
| 了解更多信息 | 1507 |
| AWSCodeDeployRoleForLambda | 1507 |
| 使用此策略 | 1507 |
| 策略详细信息 | 1508 |
| 策略版本 | 1508 |
| JSON 策略文档 | 1508 |
| 了解更多信息 | 1509 |
| AWSCodeDeployRoleForLambdaLimited | 1509 |
| 使用此策略 | 1509 |
| 策略详细信息 | 1509 |
| 策略版本 | 1510 |
| JSON 策略文档 | 1510 |
| 了解更多信息 | 1511 |
| AWSCodePipeline_FullAccess | 1511 |
| 使用此策略 | 1511 |
| 策略详细信息 | 1511 |
| 策略版本 | 1512 |
| JSON 策略文档 | 1512 |
| 了解更多信息 | 1515 |
| AWSCodePipeline_ReadOnlyAccess | 1516 |
| 使用此策略 | 1516 |
| 策略详细信息 | 1516 |
| 策略版本 | 1516 |
| JSON 策略文档 | 1516 |
| 了解更多信息 | 1517 |
| AWSCodePipelineApproverAccess | 1518 |
| 使用此策略 | 1518 |
| 策略详细信息 | 1518 |
| 策略版本 | 1518 |
| JSON 策略文档 | 1518 |
| 了解更多信息 | 1519 |

| | |
|---|------|
| AWSCodePipelineCustomActionAccess | 1519 |
| 使用此策略 | 1519 |
| 策略详细信息 | 1519 |
| 策略版本 | 1519 |
| JSON 策略文档 | 1519 |
| 了解更多信息 | 1520 |
| AWSCodeStarFullAccess | 1520 |
| 使用此策略 | 1520 |
| 策略详细信息 | 1520 |
| 策略版本 | 1521 |
| JSON 策略文档 | 1521 |
| 了解更多信息 | 1522 |
| AWSCodeStarNotificationsServiceRolePolicy | 1522 |
| 使用此策略 | 1522 |
| 策略详细信息 | 1522 |
| 策略版本 | 1522 |
| JSON 策略文档 | 1522 |
| 了解更多信息 | 1524 |
| AWSCodeStarServiceRole | 1524 |
| 使用此策略 | 1524 |
| 策略详细信息 | 1524 |
| 策略版本 | 1524 |
| JSON 策略文档 | 1524 |
| 了解更多信息 | 1529 |
| AWSCompromisedKeyQuarantine | 1529 |
| 使用此策略 | 1529 |
| 策略详细信息 | 1530 |
| 策略版本 | 1530 |
| JSON 策略文档 | 1530 |
| 了解更多信息 | 1531 |
| AWSCompromisedKeyQuarantineV2 | 1531 |
| 使用此策略 | 1531 |
| 策略详细信息 | 1531 |
| 策略版本 | 1532 |
| JSON 策略文档 | 1532 |
| 了解更多信息 | 1534 |

| | |
|--|------|
| AWSCfgMultiAccountSetupPolicy | 1534 |
| 使用此策略 | 1534 |
| 策略详细信息 | 1534 |
| 策略版本 | 1534 |
| JSON 策略文档 | 1534 |
| 了解更多信息 | 1536 |
| AWSCfgRemediationServiceRolePolicy | 1536 |
| 使用此策略 | 1537 |
| 策略详细信息 | 1537 |
| 策略版本 | 1537 |
| JSON 策略文档 | 1537 |
| 了解更多信息 | 1538 |
| AWSCfgRoleForOrganizations | 1538 |
| 使用此策略 | 1538 |
| 策略详细信息 | 1538 |
| 策略版本 | 1538 |
| JSON 策略文档 | 1538 |
| 了解更多信息 | 1539 |
| AWSCfgRulesExecutionRole | 1539 |
| 使用此策略 | 1539 |
| 策略详细信息 | 1539 |
| 策略版本 | 1540 |
| JSON 策略文档 | 1540 |
| 了解更多信息 | 1540 |
| AWSCfgServiceRolePolicy | 1541 |
| 使用此策略 | 1541 |
| 策略详细信息 | 1541 |
| 策略版本 | 1541 |
| JSON 策略文档 | 1541 |
| 了解更多信息 | 1573 |
| AWSCfgUserAccess | 1573 |
| 使用此策略 | 1573 |
| 策略详细信息 | 1573 |
| 策略版本 | 1573 |
| JSON 策略文档 | 1573 |
| 了解更多信息 | 1574 |

| | |
|---|------|
| AWSCongressConnector | 1574 |
| 使用此策略 | 1574 |
| 策略详细信息 | 1574 |
| 策略版本 | 1575 |
| JSON 策略文档 | 1575 |
| 了解更多信息 | 1577 |
| AWSCongressControlTowerAccountServiceRolePolicy | 1577 |
| 使用此策略 | 1577 |
| 策略详细信息 | 1577 |
| 策略版本 | 1577 |
| JSON 策略文档 | 1577 |
| 了解更多信息 | 1579 |
| AWSCongressControlTowerServiceRolePolicy | 1579 |
| 使用此策略 | 1579 |
| 策略详细信息 | 1579 |
| 策略版本 | 1580 |
| JSON 策略文档 | 1580 |
| 了解更多信息 | 1584 |
| AWSCongressCostAndUsageReportAutomationPolicy | 1585 |
| 使用此策略 | 1585 |
| 策略详细信息 | 1585 |
| 策略版本 | 1585 |
| JSON 策略文档 | 1585 |
| 了解更多信息 | 1586 |
| AWSCongressDataExchangeFullAccess | 1586 |
| 使用此策略 | 1587 |
| 策略详细信息 | 1587 |
| 策略版本 | 1587 |
| JSON 策略文档 | 1587 |
| 了解更多信息 | 1590 |
| AWSCongressDataExchangeProviderFullAccess | 1590 |
| 使用此策略 | 1590 |
| 策略详细信息 | 1591 |
| 策略版本 | 1591 |
| JSON 策略文档 | 1591 |
| 了解更多信息 | 1594 |

| | |
|--|------|
| AWSDataExchangeReadOnly | 1595 |
| 使用此策略 | 1595 |
| 策略详细信息 | 1595 |
| 策略版本 | 1595 |
| JSON 策略文档 | 1595 |
| 了解更多信息 | 1596 |
| AWSDataExchangeSubscriberFullAccess | 1596 |
| 使用此策略 | 1596 |
| 策略详细信息 | 1597 |
| 策略版本 | 1597 |
| JSON 策略文档 | 1597 |
| 了解更多信息 | 1599 |
| AWSDataLifecycleManagerServiceRole | 1599 |
| 使用此策略 | 1599 |
| 策略详细信息 | 1599 |
| 策略版本 | 1600 |
| JSON 策略文档 | 1600 |
| 了解更多信息 | 1601 |
| AWSDataLifecycleManagerServiceRoleForAMIManagement | 1601 |
| 使用此策略 | 1601 |
| 策略详细信息 | 1601 |
| 策略版本 | 1602 |
| JSON 策略文档 | 1602 |
| 了解更多信息 | 1603 |
| AWSDataLifecycleManagerSSMFullAccess | 1603 |
| 使用此策略 | 1603 |
| 策略详细信息 | 1603 |
| 策略版本 | 1604 |
| JSON 策略文档 | 1604 |
| 了解更多信息 | 1605 |
| AWSDataPipeline_FullAccess | 1605 |
| 使用此策略 | 1606 |
| 策略详细信息 | 1606 |
| 策略版本 | 1606 |
| JSON 策略文档 | 1606 |
| 了解更多信息 | 1607 |

| | |
|---|------|
| AWSDatapipeline_PowerUser | 1607 |
| 使用此策略 | 1607 |
| 策略详细信息 | 1607 |
| 策略版本 | 1608 |
| JSON 策略文档 | 1608 |
| 了解更多信息 | 1609 |
| AWSDatasyncDiscoveryServiceRolePolicy | 1609 |
| 使用此策略 | 1609 |
| 策略详细信息 | 1609 |
| 策略版本 | 1609 |
| JSON 策略文档 | 1609 |
| 了解更多信息 | 1610 |
| AWSDatasyncFullAccess | 1611 |
| 使用此策略 | 1611 |
| 策略详细信息 | 1611 |
| 策略版本 | 1611 |
| JSON 策略文档 | 1611 |
| 了解更多信息 | 1612 |
| AWSDatasyncReadOnlyAccess | 1613 |
| 使用此策略 | 1613 |
| 策略详细信息 | 1613 |
| 策略版本 | 1613 |
| JSON 策略文档 | 1613 |
| 了解更多信息 | 1614 |
| AWSDeepLensLambdaFunctionAccessPolicy | 1614 |
| 使用此策略 | 1614 |
| 策略详细信息 | 1614 |
| 策略版本 | 1615 |
| JSON 策略文档 | 1615 |
| 了解更多信息 | 1616 |
| AWSDeepLensServiceRolePolicy | 1616 |
| 使用此策略 | 1616 |
| 策略详细信息 | 1616 |
| 策略版本 | 1617 |
| JSON 策略文档 | 1617 |
| 了解更多信息 | 1624 |

| | |
|--|------|
| AWSDeepRacerAccountAdminAccess | 1624 |
| 使用此策略 | 1624 |
| 策略详细信息 | 1624 |
| 策略版本 | 1624 |
| JSON 策略文档 | 1625 |
| 了解更多信息 | 1625 |
| AWSDeepRacerCloudFormationAccessPolicy | 1625 |
| 使用此策略 | 1626 |
| 策略详细信息 | 1626 |
| 策略版本 | 1626 |
| JSON 策略文档 | 1626 |
| 了解更多信息 | 1629 |
| AWSDeepRacerDefaultMultiUserAccess | 1629 |
| 使用此策略 | 1629 |
| 策略详细信息 | 1629 |
| 策略版本 | 1630 |
| JSON 策略文档 | 1630 |
| 了解更多信息 | 1631 |
| AWSDeepRacerFullAccess | 1631 |
| 使用此策略 | 1631 |
| 策略详细信息 | 1632 |
| 策略版本 | 1632 |
| JSON 策略文档 | 1632 |
| 了解更多信息 | 1633 |
| AWSDeepRacerRoboMakerAccessPolicy | 1633 |
| 使用此策略 | 1633 |
| 策略详细信息 | 1633 |
| 策略版本 | 1634 |
| JSON 策略文档 | 1634 |
| 了解更多信息 | 1636 |
| AWSDeepRacerServiceRolePolicy | 1636 |
| 使用此策略 | 1636 |
| 策略详细信息 | 1636 |
| 策略版本 | 1636 |
| JSON 策略文档 | 1636 |
| 了解更多信息 | 1640 |

| | |
|--|------|
| AWSDenyAll | 1640 |
| 使用此策略 | 1640 |
| 策略详细信息 | 1640 |
| 策略版本 | 1640 |
| JSON 策略文档 | 1640 |
| 了解更多信息 | 1641 |
| AWSDeviceFarmFullAccess | 1641 |
| 使用此策略 | 1641 |
| 策略详细信息 | 1641 |
| 策略版本 | 1641 |
| JSON 策略文档 | 1642 |
| 了解更多信息 | 1642 |
| AWSDeviceFarmServiceRolePolicy | 1642 |
| 使用此策略 | 1642 |
| 策略详细信息 | 1642 |
| 策略版本 | 1643 |
| JSON 策略文档 | 1643 |
| 了解更多信息 | 1645 |
| AWSDeviceFarmTestGridServiceRolePolicy | 1645 |
| 使用此策略 | 1645 |
| 策略详细信息 | 1645 |
| 策略版本 | 1645 |
| JSON 策略文档 | 1646 |
| 了解更多信息 | 1648 |
| AWSDirectConnectFullAccess | 1648 |
| 使用此策略 | 1648 |
| 策略详细信息 | 1648 |
| 策略版本 | 1648 |
| JSON 策略文档 | 1648 |
| 了解更多信息 | 1649 |
| AWSDirectConnectReadOnlyAccess | 1649 |
| 使用此策略 | 1649 |
| 策略详细信息 | 1649 |
| 策略版本 | 1649 |
| JSON 策略文档 | 1650 |
| 了解更多信息 | 1650 |

| | |
|--|------|
| AWSDirectConnectServiceRolePolicy | 1650 |
| 使用此策略 | 1650 |
| 策略详细信息 | 1650 |
| 策略版本 | 1651 |
| JSON 策略文档 | 1651 |
| 了解更多信息 | 1651 |
| AWSDirectoryServiceFullAccess | 1651 |
| 使用此策略 | 1652 |
| 策略详细信息 | 1652 |
| 策略版本 | 1652 |
| JSON 策略文档 | 1652 |
| 了解更多信息 | 1654 |
| AWSDirectoryServiceReadOnlyAccess | 1654 |
| 使用此策略 | 1654 |
| 策略详细信息 | 1654 |
| 策略版本 | 1654 |
| JSON 策略文档 | 1655 |
| 了解更多信息 | 1655 |
| AWSDiscoveryContinuousExportFirehosePolicy | 1655 |
| 使用此策略 | 1656 |
| 策略详细信息 | 1656 |
| 策略版本 | 1656 |
| JSON 策略文档 | 1656 |
| 了解更多信息 | 1657 |
| AWSDMSFleetAdvisorServiceRolePolicy | 1657 |
| 使用此策略 | 1657 |
| 策略详细信息 | 1657 |
| 策略版本 | 1658 |
| JSON 策略文档 | 1658 |
| 了解更多信息 | 1658 |
| AWSDMSServerlessServiceRolePolicy | 1658 |
| 使用此策略 | 1658 |
| 策略详细信息 | 1659 |
| 策略版本 | 1659 |
| JSON 策略文档 | 1659 |
| 了解更多信息 | 1660 |

| | |
|---|------|
| AWSEC2CapacityReservationFleetRolePolicy | 1661 |
| 使用此策略 | 1661 |
| 策略详细信息 | 1661 |
| 策略版本 | 1661 |
| JSON 策略文档 | 1661 |
| 了解更多信息 | 1662 |
| AWSEC2FleetServiceRolePolicy | 1662 |
| 使用此策略 | 1663 |
| 策略详细信息 | 1663 |
| 策略版本 | 1663 |
| JSON 策略文档 | 1663 |
| 了解更多信息 | 1665 |
| AWSEC2SpotFleetServiceRolePolicy | 1665 |
| 使用此策略 | 1665 |
| 策略详细信息 | 1665 |
| 策略版本 | 1666 |
| JSON 策略文档 | 1666 |
| 了解更多信息 | 1668 |
| AWSEC2SpotServiceRolePolicy | 1668 |
| 使用此策略 | 1668 |
| 策略详细信息 | 1668 |
| 策略版本 | 1668 |
| JSON 策略文档 | 1668 |
| 了解更多信息 | 1670 |
| AWSECRPullThroughCache_ServiceRolePolicy | 1670 |
| 使用此策略 | 1670 |
| 策略详细信息 | 1670 |
| 策略版本 | 1670 |
| JSON 策略文档 | 1671 |
| 了解更多信息 | 1671 |
| AWSElasticBeanstalkCustomPlatformforEC2Role | 1672 |
| 使用此策略 | 1672 |
| 策略详细信息 | 1672 |
| 策略版本 | 1672 |
| JSON 策略文档 | 1672 |
| 了解更多信息 | 1674 |

| | |
|---|------|
| AWSElasticBeanstalkEnhancedHealth | 1674 |
| 使用此策略 | 1674 |
| 策略详细信息 | 1674 |
| 策略版本 | 1675 |
| JSON 策略文档 | 1675 |
| 了解更多信息 | 1676 |
| AWSElasticBeanstalkMaintenance | 1676 |
| 使用此策略 | 1676 |
| 策略详细信息 | 1676 |
| 策略版本 | 1676 |
| JSON 策略文档 | 1677 |
| 了解更多信息 | 1677 |
| AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy | 1677 |
| 使用此策略 | 1678 |
| 策略详细信息 | 1678 |
| 策略版本 | 1678 |
| JSON 策略文档 | 1678 |
| 了解更多信息 | 1685 |
| AWSElasticBeanstalkManagedUpdatesServiceRolePolicy | 1685 |
| 使用此策略 | 1685 |
| 策略详细信息 | 1685 |
| 策略版本 | 1685 |
| JSON 策略文档 | 1686 |
| 了解更多信息 | 1691 |
| AWSElasticBeanstalkMulticontainerDocker | 1691 |
| 使用此策略 | 1691 |
| 策略详细信息 | 1691 |
| 策略版本 | 1691 |
| JSON 策略文档 | 1692 |
| 了解更多信息 | 1693 |
| AWSElasticBeanstalkReadOnly | 1693 |
| 使用此策略 | 1693 |
| 策略详细信息 | 1693 |
| 策略版本 | 1693 |
| JSON 策略文档 | 1693 |
| 了解更多信息 | 1695 |

| | |
|---|------|
| AWSElasticBeanstalkRoleCore | 1696 |
| 使用此策略 | 1696 |
| 策略详细信息 | 1696 |
| 策略版本 | 1696 |
| JSON 策略文档 | 1696 |
| 了解更多信息 | 1701 |
| AWSElasticBeanstalkRoleCWL | 1701 |
| 使用此策略 | 1701 |
| 策略详细信息 | 1702 |
| 策略版本 | 1702 |
| JSON 策略文档 | 1702 |
| 了解更多信息 | 1702 |
| AWSElasticBeanstalkRoleECS | 1703 |
| 使用此策略 | 1703 |
| 策略详细信息 | 1703 |
| 策略版本 | 1703 |
| JSON 策略文档 | 1703 |
| 了解更多信息 | 1704 |
| AWSElasticBeanstalkRoleRDS | 1704 |
| 使用此策略 | 1704 |
| 策略详细信息 | 1704 |
| 策略版本 | 1705 |
| JSON 策略文档 | 1705 |
| 了解更多信息 | 1705 |
| AWSElasticBeanstalkRoleSNS | 1706 |
| 使用此策略 | 1706 |
| 策略详细信息 | 1706 |
| 策略版本 | 1706 |
| JSON 策略文档 | 1706 |
| 了解更多信息 | 1707 |
| AWSElasticBeanstalkRoleWorkerTier | 1707 |
| 使用此策略 | 1707 |
| 策略详细信息 | 1707 |
| 策略版本 | 1708 |
| JSON 策略文档 | 1708 |
| 了解更多信息 | 1708 |

| | |
|---|------|
| AWSElasticBeanstalkService | 1709 |
| 使用此策略 | 1709 |
| 策略详细信息 | 1709 |
| 策略版本 | 1709 |
| JSON 策略文档 | 1709 |
| 了解更多信息 | 1714 |
| AWSElasticBeanstalkServiceRolePolicy | 1714 |
| 使用此策略 | 1714 |
| 策略详细信息 | 1714 |
| 策略版本 | 1714 |
| JSON 策略文档 | 1714 |
| 了解更多信息 | 1716 |
| AWSElasticBeanstalkWebTier | 1716 |
| 使用此策略 | 1716 |
| 策略详细信息 | 1716 |
| 策略版本 | 1716 |
| JSON 策略文档 | 1717 |
| 了解更多信息 | 1718 |
| AWSElasticBeanstalkWorkerTier | 1718 |
| 使用此策略 | 1718 |
| 策略详细信息 | 1718 |
| 策略版本 | 1719 |
| JSON 策略文档 | 1719 |
| 了解更多信息 | 1721 |
| AWSElasticDisasterRecoveryAgentInstallationPolicy | 1721 |
| 使用此策略 | 1721 |
| 策略详细信息 | 1721 |
| 策略版本 | 1722 |
| JSON 策略文档 | 1722 |
| 了解更多信息 | 1723 |
| AWSElasticDisasterRecoveryAgentPolicy | 1723 |
| 使用此策略 | 1724 |
| 策略详细信息 | 1724 |
| 策略版本 | 1724 |
| JSON 策略文档 | 1724 |
| 了解更多信息 | 1725 |

| | |
|---|------|
| AWSElasticDisasterRecoveryConsoleFullAccess | 1725 |
| 使用此策略 | 1725 |
| 策略详细信息 | 1725 |
| 策略版本 | 1726 |
| JSON 策略文档 | 1726 |
| 了解更多信息 | 1735 |
| AWSElasticDisasterRecoveryConsoleFullAccess_v2 | 1736 |
| 使用此策略 | 1736 |
| 策略详细信息 | 1736 |
| 策略版本 | 1736 |
| JSON 策略文档 | 1736 |
| 了解更多信息 | 1749 |
| AWSElasticDisasterRecoveryConversionServerPolicy | 1749 |
| 使用此策略 | 1749 |
| 策略详细信息 | 1749 |
| 策略版本 | 1750 |
| JSON 策略文档 | 1750 |
| 了解更多信息 | 1750 |
| AWSElasticDisasterRecoveryCrossAccountReplicationPolicy | 1751 |
| 使用此策略 | 1751 |
| 策略详细信息 | 1751 |
| 策略版本 | 1751 |
| JSON 策略文档 | 1751 |
| 了解更多信息 | 1752 |
| AWSElasticDisasterRecoveryEc2InstancePolicy | 1752 |
| 使用此策略 | 1752 |
| 策略详细信息 | 1752 |
| 策略版本 | 1753 |
| JSON 策略文档 | 1753 |
| 了解更多信息 | 1755 |
| AWSElasticDisasterRecoveryFailbackInstallationPolicy | 1755 |
| 使用此策略 | 1755 |
| 策略详细信息 | 1755 |
| 策略版本 | 1756 |
| JSON 策略文档 | 1756 |
| 了解更多信息 | 1756 |

| | |
|--|------|
| AWSElasticDisasterRecoveryFailbackPolicy | 1757 |
| 使用此策略 | 1757 |
| 策略详细信息 | 1757 |
| 策略版本 | 1757 |
| JSON 策略文档 | 1757 |
| 了解更多信息 | 1759 |
| AWSElasticDisasterRecoveryLaunchActionsPolicy | 1759 |
| 使用此策略 | 1759 |
| 策略详细信息 | 1759 |
| 策略版本 | 1759 |
| JSON 策略文档 | 1759 |
| 了解更多信息 | 1765 |
| AWSElasticDisasterRecoveryNetworkReplicationPolicy | 1766 |
| 使用此策略 | 1766 |
| 策略详细信息 | 1766 |
| 策略版本 | 1766 |
| JSON 策略文档 | 1766 |
| 了解更多信息 | 1767 |
| AWSElasticDisasterRecoveryReadOnlyAccess | 1767 |
| 使用此策略 | 1767 |
| 策略详细信息 | 1767 |
| 策略版本 | 1768 |
| JSON 策略文档 | 1768 |
| 了解更多信息 | 1770 |
| AWSElasticDisasterRecoveryRecoveryInstancePolicy | 1770 |
| 使用此策略 | 1770 |
| 策略详细信息 | 1770 |
| 策略版本 | 1771 |
| JSON 策略文档 | 1771 |
| 了解更多信息 | 1773 |
| AWSElasticDisasterRecoveryReplicationServerPolicy | 1773 |
| 使用此策略 | 1774 |
| 策略详细信息 | 1774 |
| 策略版本 | 1774 |
| JSON 策略文档 | 1774 |
| 了解更多信息 | 1776 |

| | |
|---|------|
| AWSElasticDisasterRecoveryServiceRolePolicy | 1777 |
| 使用此策略 | 1777 |
| 策略详细信息 | 1777 |
| 策略版本 | 1777 |
| JSON 策略文档 | 1777 |
| 了解更多信息 | 1786 |
| AWSElasticDisasterRecoveryStagingAccountPolicy | 1786 |
| 使用此策略 | 1786 |
| 策略详细信息 | 1786 |
| 策略版本 | 1786 |
| JSON 策略文档 | 1786 |
| 了解更多信息 | 1787 |
| AWSElasticDisasterRecoveryStagingAccountPolicy_v2 | 1788 |
| 使用此策略 | 1788 |
| 策略详细信息 | 1788 |
| 策略版本 | 1788 |
| JSON 策略文档 | 1788 |
| 了解更多信息 | 1789 |
| AWSElasticLoadBalancingClassicServiceRolePolicy | 1790 |
| 使用此策略 | 1790 |
| 策略详细信息 | 1790 |
| 策略版本 | 1790 |
| JSON 策略文档 | 1790 |
| 了解更多信息 | 1791 |
| AWSElasticLoadBalancingServiceRolePolicy | 1791 |
| 使用此策略 | 1791 |
| 策略详细信息 | 1791 |
| 策略版本 | 1792 |
| JSON 策略文档 | 1792 |
| 了解更多信息 | 1793 |
| AWSElementalMediaConvertFullAccess | 1793 |
| 使用此策略 | 1793 |
| 策略详细信息 | 1793 |
| 策略版本 | 1794 |
| JSON 策略文档 | 1794 |
| 了解更多信息 | 1794 |

| | |
|--|------|
| AWSElementalMediaConvertReadOnly | 1795 |
| 使用此策略 | 1795 |
| 策略详细信息 | 1795 |
| 策略版本 | 1795 |
| JSON 策略文档 | 1795 |
| 了解更多信息 | 1796 |
| AWSElementalMediaLiveFullAccess | 1796 |
| 使用此策略 | 1796 |
| 策略详细信息 | 1796 |
| 策略版本 | 1796 |
| JSON 策略文档 | 1797 |
| 了解更多信息 | 1797 |
| AWSElementalMediaLiveReadOnly | 1797 |
| 使用此策略 | 1797 |
| 策略详细信息 | 1797 |
| 策略版本 | 1797 |
| JSON 策略文档 | 1798 |
| 了解更多信息 | 1798 |
| AWSElementalMediaPackageFullAccess | 1798 |
| 使用此策略 | 1798 |
| 策略详细信息 | 1798 |
| 策略版本 | 1799 |
| JSON 策略文档 | 1799 |
| 了解更多信息 | 1799 |
| AWSElementalMediaPackageReadOnly | 1799 |
| 使用此策略 | 1799 |
| 策略详细信息 | 1800 |
| 策略版本 | 1800 |
| JSON 策略文档 | 1800 |
| 了解更多信息 | 1800 |
| AWSElementalMediaPackageV2FullAccess | 1801 |
| 使用此策略 | 1801 |
| 策略详细信息 | 1801 |
| 策略版本 | 1801 |
| JSON 策略文档 | 1801 |
| 了解更多信息 | 1801 |

| | |
|---|------|
| AWSElementalMediaPackageV2ReadOnly | 1802 |
| 使用此策略 | 1802 |
| 策略详细信息 | 1802 |
| 策略版本 | 1802 |
| JSON 策略文档 | 1802 |
| 了解更多信息 | 1803 |
| AWSElementalMediaStoreFullAccess | 1803 |
| 使用此策略 | 1803 |
| 策略详细信息 | 1803 |
| 策略版本 | 1803 |
| JSON 策略文档 | 1803 |
| 了解更多信息 | 1804 |
| AWSElementalMediaStoreReadOnly | 1804 |
| 使用此策略 | 1804 |
| 策略详细信息 | 1804 |
| 策略版本 | 1805 |
| JSON 策略文档 | 1805 |
| 了解更多信息 | 1805 |
| AWSElementalMediaTailorFullAccess | 1806 |
| 使用此策略 | 1806 |
| 策略详细信息 | 1806 |
| 策略版本 | 1806 |
| JSON 策略文档 | 1806 |
| 了解更多信息 | 1806 |
| AWSElementalMediaTailorReadOnly | 1807 |
| 使用此策略 | 1807 |
| 策略详细信息 | 1807 |
| 策略版本 | 1807 |
| JSON 策略文档 | 1807 |
| 了解更多信息 | 1808 |
| AWSEnhancedClassicNetworkingMangementPolicy | 1808 |
| 使用此策略 | 1808 |
| 策略详细信息 | 1808 |
| 策略版本 | 1808 |
| JSON 策略文档 | 1808 |
| 了解更多信息 | 1809 |

| | |
|--|------|
| AWSEntityResolutionConsoleFullAccess | 1809 |
| 使用此策略 | 1809 |
| 策略详细信息 | 1809 |
| 策略版本 | 1809 |
| JSON 策略文档 | 1810 |
| 了解更多信息 | 1812 |
| AWSEntityResolutionConsoleReadOnlyAccess | 1813 |
| 使用此策略 | 1813 |
| 策略详细信息 | 1813 |
| 策略版本 | 1813 |
| JSON 策略文档 | 1813 |
| 了解更多信息 | 1814 |
| AWSFaultInjectionSimulatorEC2Access | 1814 |
| 使用此策略 | 1814 |
| 策略详细信息 | 1814 |
| 策略版本 | 1814 |
| JSON 策略文档 | 1814 |
| 了解更多信息 | 1816 |
| AWSFaultInjectionSimulatorECSAccess | 1816 |
| 使用此策略 | 1816 |
| 策略详细信息 | 1816 |
| 策略版本 | 1817 |
| JSON 策略文档 | 1817 |
| 了解更多信息 | 1818 |
| AWSFaultInjectionSimulatorEKSAccess | 1819 |
| 使用此策略 | 1819 |
| 策略详细信息 | 1819 |
| 策略版本 | 1819 |
| JSON 策略文档 | 1819 |
| 了解更多信息 | 1820 |
| AWSFaultInjectionSimulatorNetworkAccess | 1821 |
| 使用此策略 | 1821 |
| 策略详细信息 | 1821 |
| 策略版本 | 1821 |
| JSON 策略文档 | 1821 |
| 了解更多信息 | 1828 |

| | |
|---|------|
| AWSFaultInjectionSimulatorRDSAccess | 1828 |
| 使用此策略 | 1828 |
| 策略详细信息 | 1828 |
| 策略版本 | 1829 |
| JSON 策略文档 | 1829 |
| 了解更多信息 | 1830 |
| AWSFaultInjectionSimulatorSSMAccess | 1830 |
| 使用此策略 | 1830 |
| 策略详细信息 | 1830 |
| 策略版本 | 1831 |
| JSON 策略文档 | 1831 |
| 了解更多信息 | 1832 |
| AWSFinSpaceServiceRolePolicy | 1832 |
| 使用此策略 | 1832 |
| 策略详细信息 | 1832 |
| 策略版本 | 1833 |
| JSON 策略文档 | 1833 |
| 了解更多信息 | 1833 |
| AWSFMAdminFullAccess | 1834 |
| 使用此策略 | 1834 |
| 策略详细信息 | 1834 |
| 策略版本 | 1834 |
| JSON 策略文档 | 1834 |
| 了解更多信息 | 1836 |
| AWSFMAdminReadOnlyAccess | 1836 |
| 使用此策略 | 1836 |
| 策略详细信息 | 1836 |
| 策略版本 | 1837 |
| JSON 策略文档 | 1837 |
| 了解更多信息 | 1838 |
| AWSFMMemberReadOnlyAccess | 1838 |
| 使用此策略 | 1839 |
| 策略详细信息 | 1839 |
| 策略版本 | 1839 |
| JSON 策略文档 | 1839 |
| 了解更多信息 | 1840 |

| | |
|---|------|
| AWSForWordPressPluginPolicy | 1840 |
| 使用此策略 | 1840 |
| 策略详细信息 | 1840 |
| 策略版本 | 1840 |
| JSON 策略文档 | 1840 |
| 了解更多信息 | 1842 |
| AWSGitSyncServiceRolePolicy | 1842 |
| 使用此策略 | 1842 |
| 策略详细信息 | 1843 |
| 策略版本 | 1843 |
| JSON 策略文档 | 1843 |
| 了解更多信息 | 1843 |
| AWSGlobalAcceleratorSLRPolicy | 1844 |
| 使用此策略 | 1844 |
| 策略详细信息 | 1844 |
| 策略版本 | 1844 |
| JSON 策略文档 | 1844 |
| 了解更多信息 | 1846 |
| AWSGlueConsoleFullAccess | 1846 |
| 使用此策略 | 1846 |
| 策略详细信息 | 1846 |
| 策略版本 | 1846 |
| JSON 策略文档 | 1846 |
| 了解更多信息 | 1851 |
| AWSGlueConsoleSageMakerNotebookFullAccess | 1851 |
| 使用此策略 | 1851 |
| 策略详细信息 | 1851 |
| 策略版本 | 1851 |
| JSON 策略文档 | 1851 |
| 了解更多信息 | 1857 |
| AwsGlueDataBrewFullAccessPolicy | 1857 |
| 使用此策略 | 1857 |
| 策略详细信息 | 1857 |
| 策略版本 | 1857 |
| JSON 策略文档 | 1857 |
| 了解更多信息 | 1862 |

| | |
|--|------|
| AWSGlueDataBrewServiceRole | 1863 |
| 使用此策略 | 1863 |
| 策略详细信息 | 1863 |
| 策略版本 | 1863 |
| JSON 策略文档 | 1863 |
| 了解更多信息 | 1866 |
| AWSGlueSchemaRegistryFullAccess | 1866 |
| 使用此策略 | 1866 |
| 策略详细信息 | 1866 |
| 策略版本 | 1867 |
| JSON 策略文档 | 1867 |
| 了解更多信息 | 1868 |
| AWSGlueSchemaRegistryReadOnlyAccess | 1868 |
| 使用此策略 | 1868 |
| 策略详细信息 | 1868 |
| 策略版本 | 1869 |
| JSON 策略文档 | 1869 |
| 了解更多信息 | 1869 |
| AWSGlueServiceNotebookRole | 1870 |
| 使用此策略 | 1870 |
| 策略详细信息 | 1870 |
| 策略版本 | 1870 |
| JSON 策略文档 | 1870 |
| 了解更多信息 | 1873 |
| AWSGlueServiceRole | 1873 |
| 使用此策略 | 1873 |
| 策略详细信息 | 1873 |
| 策略版本 | 1873 |
| JSON 策略文档 | 1873 |
| 了解更多信息 | 1876 |
| AwsGlueSessionUserRestrictedNotebookPolicy | 1876 |
| 使用此策略 | 1876 |
| 策略详细信息 | 1876 |
| 策略版本 | 1876 |
| JSON 策略文档 | 1876 |
| 了解更多信息 | 1879 |

| | |
|---|------|
| AwsGlueSessionUserRestrictedNotebookServiceRole | 1879 |
| 使用此策略 | 1879 |
| 策略详细信息 | 1879 |
| 策略版本 | 1880 |
| JSON 策略文档 | 1880 |
| 了解更多信息 | 1883 |
| AwsGlueSessionUserRestrictedPolicy | 1884 |
| 使用此策略 | 1884 |
| 策略详细信息 | 1884 |
| 策略版本 | 1884 |
| JSON 策略文档 | 1884 |
| 了解更多信息 | 1886 |
| AwsGlueSessionUserRestrictedServiceRole | 1887 |
| 使用此策略 | 1887 |
| 策略详细信息 | 1887 |
| 策略版本 | 1887 |
| JSON 策略文档 | 1887 |
| 了解更多信息 | 1891 |
| AWSGrafanaAccountAdministrator | 1891 |
| 使用此策略 | 1891 |
| 策略详细信息 | 1891 |
| 策略版本 | 1891 |
| JSON 策略文档 | 1892 |
| 了解更多信息 | 1893 |
| AWSGrafanaConsoleReadOnlyAccess | 1893 |
| 使用此策略 | 1893 |
| 策略详细信息 | 1893 |
| 策略版本 | 1893 |
| JSON 策略文档 | 1893 |
| 了解更多信息 | 1894 |
| AWSGrafanaWorkspacePermissionManagement | 1894 |
| 使用此策略 | 1894 |
| 策略详细信息 | 1894 |
| 策略版本 | 1894 |
| JSON 策略文档 | 1895 |
| 了解更多信息 | 1896 |

| | |
|---|------|
| AWSGrafanaWorkspacePermissionManagementV2 | 1896 |
| 使用此策略 | 1896 |
| 策略详细信息 | 1896 |
| 策略版本 | 1896 |
| JSON 策略文档 | 1896 |
| 了解更多信息 | 1897 |
| AWSGreengrassFullAccess | 1897 |
| 使用此策略 | 1898 |
| 策略详细信息 | 1898 |
| 策略版本 | 1898 |
| JSON 策略文档 | 1898 |
| 了解更多信息 | 1898 |
| AWSGreengrassReadOnlyAccess | 1899 |
| 使用此策略 | 1899 |
| 策略详细信息 | 1899 |
| 策略版本 | 1899 |
| JSON 策略文档 | 1899 |
| 了解更多信息 | 1900 |
| AWSGreengrassResourceAccessRolePolicy | 1900 |
| 使用此策略 | 1900 |
| 策略详细信息 | 1900 |
| 策略版本 | 1900 |
| JSON 策略文档 | 1901 |
| 了解更多信息 | 1903 |
| AWSGroundStationAgentInstancePolicy | 1903 |
| 使用此策略 | 1903 |
| 策略详细信息 | 1903 |
| 策略版本 | 1903 |
| JSON 策略文档 | 1904 |
| 了解更多信息 | 1904 |
| AWSHealth_EventProcessorServiceRolePolicy | 1904 |
| 使用此策略 | 1904 |
| 策略详细信息 | 1904 |
| 策略版本 | 1905 |
| JSON 策略文档 | 1905 |
| 了解更多信息 | 1906 |

| | |
|---|------|
| AWSHealthFullAccess | 1906 |
| 使用此策略 | 1906 |
| 策略详细信息 | 1906 |
| 策略版本 | 1906 |
| JSON 策略文档 | 1906 |
| 了解更多信息 | 1907 |
| AWSHealthImagingFullAccess | 1908 |
| 使用此策略 | 1908 |
| 策略详细信息 | 1908 |
| 策略版本 | 1908 |
| JSON 策略文档 | 1908 |
| 了解更多信息 | 1909 |
| AWSHealthImagingReadOnlyAccess | 1909 |
| 使用此策略 | 1909 |
| 策略详细信息 | 1909 |
| 策略版本 | 1909 |
| JSON 策略文档 | 1910 |
| 了解更多信息 | 1910 |
| AWSIAMIdentityCenterAllowListForIdentityContext | 1910 |
| 使用此策略 | 1911 |
| 策略详细信息 | 1911 |
| 策略版本 | 1911 |
| JSON 策略文档 | 1911 |
| 了解更多信息 | 1913 |
| AWSIdentitySyncFullAccess | 1913 |
| 使用此策略 | 1913 |
| 策略详细信息 | 1913 |
| 策略版本 | 1913 |
| JSON 策略文档 | 1914 |
| 了解更多信息 | 1914 |
| AWSIdentitySyncReadOnlyAccess | 1915 |
| 使用此策略 | 1915 |
| 策略详细信息 | 1915 |
| 策略版本 | 1915 |
| JSON 策略文档 | 1915 |
| 了解更多信息 | 1916 |

| | |
|---|------|
| AWSImageBuilderFullAccess | 1916 |
| 使用此策略 | 1916 |
| 策略详细信息 | 1916 |
| 策略版本 | 1916 |
| JSON 策略文档 | 1917 |
| 了解更多信息 | 1919 |
| AWSImageBuilderReadOnlyAccess | 1919 |
| 使用此策略 | 1920 |
| 策略详细信息 | 1920 |
| 策略版本 | 1920 |
| JSON 策略文档 | 1920 |
| 了解更多信息 | 1921 |
| AWSImportExportFullAccess | 1921 |
| 使用此策略 | 1921 |
| 策略详细信息 | 1921 |
| 策略版本 | 1921 |
| JSON 策略文档 | 1921 |
| 了解更多信息 | 1922 |
| AWSImportExportReadOnlyAccess | 1922 |
| 使用此策略 | 1922 |
| 策略详细信息 | 1922 |
| 策略版本 | 1922 |
| JSON 策略文档 | 1923 |
| 了解更多信息 | 1923 |
| AWSIncidentManagerIncidentAccessServiceRolePolicy | 1923 |
| 使用此策略 | 1923 |
| 策略详细信息 | 1923 |
| 策略版本 | 1924 |
| JSON 策略文档 | 1924 |
| 了解更多信息 | 1924 |
| AWSIncidentManagerResolverAccess | 1925 |
| 使用此策略 | 1925 |
| 策略详细信息 | 1925 |
| 策略版本 | 1925 |
| JSON 策略文档 | 1925 |
| 了解更多信息 | 1926 |

| | |
|---|------|
| AWSIncidentManagerServiceRolePolicy | 1926 |
| 使用此策略 | 1927 |
| 策略详细信息 | 1927 |
| 策略版本 | 1927 |
| JSON 策略文档 | 1927 |
| 了解更多信息 | 1928 |
| AWSIoT1ClickFullAccess | 1928 |
| 使用此策略 | 1928 |
| 策略详细信息 | 1928 |
| 策略版本 | 1929 |
| JSON 策略文档 | 1929 |
| 了解更多信息 | 1929 |
| AWSIoT1ClickReadOnlyAccess | 1929 |
| 使用此策略 | 1930 |
| 策略详细信息 | 1930 |
| 策略版本 | 1930 |
| JSON 策略文档 | 1930 |
| 了解更多信息 | 1930 |
| AWSIoTAnalyticsFullAccess | 1931 |
| 使用此策略 | 1931 |
| 策略详细信息 | 1931 |
| 策略版本 | 1931 |
| JSON 策略文档 | 1931 |
| 了解更多信息 | 1932 |
| AWSIoTAnalyticsReadOnlyAccess | 1932 |
| 使用此策略 | 1932 |
| 策略详细信息 | 1932 |
| 策略版本 | 1932 |
| JSON 策略文档 | 1932 |
| 了解更多信息 | 1933 |
| AWSIoTConfigAccess | 1933 |
| 使用此策略 | 1933 |
| 策略详细信息 | 1933 |
| 策略版本 | 1933 |
| JSON 策略文档 | 1934 |
| 了解更多信息 | 1937 |

| | |
|---|------|
| AWSIoTConfigReadOnlyAccess | 1938 |
| 使用此策略 | 1938 |
| 策略详细信息 | 1938 |
| 策略版本 | 1938 |
| JSON 策略文档 | 1938 |
| 了解更多信息 | 1940 |
| AWSIoTDataAccess | 1940 |
| 使用此策略 | 1940 |
| 策略详细信息 | 1941 |
| 策略版本 | 1941 |
| JSON 策略文档 | 1941 |
| 了解更多信息 | 1941 |
| AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction | 1942 |
| 使用此策略 | 1942 |
| 策略详细信息 | 1942 |
| 策略版本 | 1942 |
| JSON 策略文档 | 1942 |
| 了解更多信息 | 1943 |
| AWSIoTDeviceDefenderAudit | 1943 |
| 使用此策略 | 1943 |
| 策略详细信息 | 1943 |
| 策略版本 | 1943 |
| JSON 策略文档 | 1944 |
| 了解更多信息 | 1944 |
| AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction | 1945 |
| 使用此策略 | 1945 |
| 策略详细信息 | 1945 |
| 策略版本 | 1945 |
| JSON 策略文档 | 1945 |
| 了解更多信息 | 1946 |
| AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction | 1946 |
| 使用此策略 | 1946 |
| 策略详细信息 | 1947 |
| 策略版本 | 1947 |
| JSON 策略文档 | 1947 |
| 了解更多信息 | 1947 |

| | |
|--|------|
| AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction | 1948 |
| 使用此策略 | 1948 |
| 策略详细信息 | 1948 |
| 策略版本 | 1948 |
| JSON 策略文档 | 1948 |
| 了解更多信息 | 1949 |
| AWSIoTDeviceDefenderUpdateCACertMitigationAction | 1949 |
| 使用此策略 | 1949 |
| 策略详细信息 | 1949 |
| 策略版本 | 1949 |
| JSON 策略文档 | 1949 |
| 了解更多信息 | 1950 |
| AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction | 1950 |
| 使用此策略 | 1950 |
| 策略详细信息 | 1950 |
| 策略版本 | 1951 |
| JSON 策略文档 | 1951 |
| 了解更多信息 | 1951 |
| AWSIoTDeviceTesterForFreeRTOSFullAccess | 1951 |
| 使用此策略 | 1951 |
| 策略详细信息 | 1952 |
| 策略版本 | 1952 |
| JSON 策略文档 | 1952 |
| 了解更多信息 | 1958 |
| AWSIoTDeviceTesterForGreengrassFullAccess | 1958 |
| 使用此策略 | 1958 |
| 策略详细信息 | 1958 |
| 策略版本 | 1959 |
| JSON 策略文档 | 1959 |
| 了解更多信息 | 1962 |
| AWSIoTEventsFullAccess | 1962 |
| 使用此策略 | 1962 |
| 策略详细信息 | 1962 |
| 策略版本 | 1962 |
| JSON 策略文档 | 1963 |
| 了解更多信息 | 1963 |

| | |
|--|------|
| AWSIoTEventsReadOnlyAccess | 1963 |
| 使用此策略 | 1963 |
| 策略详细信息 | 1963 |
| 策略版本 | 1964 |
| JSON 策略文档 | 1964 |
| 了解更多信息 | 1964 |
| AWSIoTFleetHubFederationAccess | 1964 |
| 使用此策略 | 1964 |
| 策略详细信息 | 1965 |
| 策略版本 | 1965 |
| JSON 策略文档 | 1965 |
| 了解更多信息 | 1967 |
| AWSIoTFleetwiseServiceRolePolicy | 1967 |
| 使用此策略 | 1967 |
| 策略详细信息 | 1967 |
| 策略版本 | 1967 |
| JSON 策略文档 | 1967 |
| 了解更多信息 | 1968 |
| AWSIoTFullAccess | 1968 |
| 使用此策略 | 1968 |
| 策略详细信息 | 1968 |
| 策略版本 | 1969 |
| JSON 策略文档 | 1969 |
| 了解更多信息 | 1969 |
| AWSIoTLogging | 1969 |
| 使用此策略 | 1969 |
| 策略详细信息 | 1970 |
| 策略版本 | 1970 |
| JSON 策略文档 | 1970 |
| 了解更多信息 | 1970 |
| AWSIoTOTAUpdate | 1971 |
| 使用此策略 | 1971 |
| 策略详细信息 | 1971 |
| 策略版本 | 1971 |
| JSON 策略文档 | 1971 |
| 了解更多信息 | 1972 |

| | |
|---|------|
| AWSIoTRoboRunnerFullAccess | 1972 |
| 使用此策略 | 1972 |
| 策略详细信息 | 1972 |
| 策略版本 | 1972 |
| JSON 策略文档 | 1972 |
| 了解更多信息 | 1973 |
| AWSIoTRoboRunnerReadOnly | 1973 |
| 使用此策略 | 1973 |
| 策略详细信息 | 1973 |
| 策略版本 | 1974 |
| JSON 策略文档 | 1974 |
| 了解更多信息 | 1974 |
| AWSIoTRoboRunnerServiceRolePolicy | 1975 |
| 使用此策略 | 1975 |
| 策略详细信息 | 1975 |
| 策略版本 | 1975 |
| JSON 策略文档 | 1975 |
| 了解更多信息 | 1976 |
| AWSIoTRuleActions | 1976 |
| 使用此策略 | 1976 |
| 策略详细信息 | 1976 |
| 策略版本 | 1976 |
| JSON 策略文档 | 1976 |
| 了解更多信息 | 1977 |
| AWSIoTSiteWiseConsoleFullAccess | 1977 |
| 使用此策略 | 1977 |
| 策略详细信息 | 1977 |
| 策略版本 | 1978 |
| JSON 策略文档 | 1978 |
| 了解更多信息 | 1980 |
| AWSIoTSiteWiseFullAccess | 1980 |
| 使用此策略 | 1980 |
| 策略详细信息 | 1980 |
| 策略版本 | 1980 |
| JSON 策略文档 | 1981 |
| 了解更多信息 | 1981 |

| | |
|--|------|
| AWSIoTSiteWiseMonitorPortalAccess | 1981 |
| 使用此策略 | 1981 |
| 策略详细信息 | 1981 |
| 策略版本 | 1982 |
| JSON 策略文档 | 1982 |
| 了解更多信息 | 1983 |
| AWSIoTSiteWiseMonitorServiceRolePolicy | 1983 |
| 使用此策略 | 1983 |
| 策略详细信息 | 1983 |
| 策略版本 | 1983 |
| JSON 策略文档 | 1984 |
| 了解更多信息 | 1985 |
| AWSIoTSiteWiseReadOnlyAccess | 1985 |
| 使用此策略 | 1985 |
| 策略详细信息 | 1985 |
| 策略版本 | 1985 |
| JSON 策略文档 | 1985 |
| 了解更多信息 | 1986 |
| AWSIoTThingsRegistration | 1986 |
| 使用此策略 | 1986 |
| 策略详细信息 | 1986 |
| 策略版本 | 1986 |
| JSON 策略文档 | 1987 |
| 了解更多信息 | 1988 |
| AWSIoTThingMakerServiceRolePolicy | 1988 |
| 使用此策略 | 1988 |
| 策略详细信息 | 1988 |
| 策略版本 | 1988 |
| JSON 策略文档 | 1989 |
| 了解更多信息 | 1990 |
| AWSIoTWirelessDataAccess | 1990 |
| 使用此策略 | 1990 |
| 策略详细信息 | 1990 |
| 策略版本 | 1991 |
| JSON 策略文档 | 1991 |
| 了解更多信息 | 1991 |

| | |
|--|------|
| AWSIoTWirelessFullAccess | 1991 |
| 使用此策略 | 1992 |
| 策略详细信息 | 1992 |
| 策略版本 | 1992 |
| JSON 策略文档 | 1992 |
| 了解更多信息 | 1992 |
| AWSIoTWirelessFullPublishAccess | 1993 |
| 使用此策略 | 1993 |
| 策略详细信息 | 1993 |
| 策略版本 | 1993 |
| JSON 策略文档 | 1993 |
| 了解更多信息 | 1994 |
| AWSIoTWirelessGatewayCertManager | 1994 |
| 使用此策略 | 1994 |
| 策略详细信息 | 1994 |
| 策略版本 | 1994 |
| JSON 策略文档 | 1994 |
| 了解更多信息 | 1995 |
| AWSIoTWirelessLogging | 1995 |
| 使用此策略 | 1995 |
| 策略详细信息 | 1995 |
| 策略版本 | 1996 |
| JSON 策略文档 | 1996 |
| 了解更多信息 | 1996 |
| AWSIoTWirelessReadOnlyAccess | 1996 |
| 使用此策略 | 1997 |
| 策略详细信息 | 1997 |
| 策略版本 | 1997 |
| JSON 策略文档 | 1997 |
| 了解更多信息 | 1997 |
| AWSIPAMServiceRolePolicy | 1998 |
| 使用此策略 | 1998 |
| 策略详细信息 | 1998 |
| 策略版本 | 1998 |
| JSON 策略文档 | 1998 |
| 了解更多信息 | 1999 |

| | |
|---|------|
| AWSIQContractServiceRolePolicy | 1999 |
| 使用此策略 | 2000 |
| 策略详细信息 | 2000 |
| 策略版本 | 2000 |
| JSON 策略文档 | 2000 |
| 了解更多信息 | 2000 |
| AWSIQFullAccess | 2001 |
| 使用此策略 | 2001 |
| 策略详细信息 | 2001 |
| 策略版本 | 2001 |
| JSON 策略文档 | 2001 |
| 了解更多信息 | 2002 |
| AWSIQPermissionServiceRolePolicy | 2002 |
| 使用此策略 | 2002 |
| 策略详细信息 | 2002 |
| 策略版本 | 2003 |
| JSON 策略文档 | 2003 |
| 了解更多信息 | 2004 |
| AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy | 2004 |
| 使用此策略 | 2004 |
| 策略详细信息 | 2004 |
| 策略版本 | 2004 |
| JSON 策略文档 | 2004 |
| 了解更多信息 | 2005 |
| AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy | 2005 |
| 使用此策略 | 2005 |
| 策略详细信息 | 2005 |
| 策略版本 | 2006 |
| JSON 策略文档 | 2006 |
| 了解更多信息 | 2006 |
| AWSKeyManagementServicePowerUser | 2006 |
| 使用此策略 | 2006 |
| 策略详细信息 | 2006 |
| 策略版本 | 2007 |
| JSON 策略文档 | 2007 |
| 了解更多信息 | 2007 |

| | |
|---|------|
| AWSLakeFormationCrossAccountManager | 2008 |
| 使用此策略 | 2008 |
| 策略详细信息 | 2008 |
| 策略版本 | 2008 |
| JSON 策略文档 | 2008 |
| 了解更多信息 | 2010 |
| AWSLakeFormationDataAdmin | 2010 |
| 使用此策略 | 2010 |
| 策略详细信息 | 2010 |
| 策略版本 | 2011 |
| JSON 策略文档 | 2011 |
| 了解更多信息 | 2012 |
| AWSLambda_FullAccess | 2012 |
| 使用此策略 | 2012 |
| 策略详细信息 | 2013 |
| 策略版本 | 2013 |
| JSON 策略文档 | 2013 |
| 了解更多信息 | 2014 |
| AWSLambda_ReadOnlyAccess | 2014 |
| 使用此策略 | 2015 |
| 策略详细信息 | 2015 |
| 策略版本 | 2015 |
| JSON 策略文档 | 2015 |
| 了解更多信息 | 2016 |
| AWSLambdaBasicExecutionRole | 2016 |
| 使用此策略 | 2017 |
| 策略详细信息 | 2017 |
| 策略版本 | 2017 |
| JSON 策略文档 | 2017 |
| 了解更多信息 | 2017 |
| AWSLambdaDynamoDBExecutionRole | 2018 |
| 使用此策略 | 2018 |
| 策略详细信息 | 2018 |
| 策略版本 | 2018 |
| JSON 策略文档 | 2018 |
| 了解更多信息 | 2019 |

| | |
|-------------------------------------|------|
| AWSLambdaENIManagementAccess | 2019 |
| 使用此策略 | 2019 |
| 策略详细信息 | 2019 |
| 策略版本 | 2019 |
| JSON 策略文档 | 2020 |
| 了解更多信息 | 2020 |
| AWSLambdaExecute | 2020 |
| 使用此策略 | 2020 |
| 策略详细信息 | 2020 |
| 策略版本 | 2021 |
| JSON 策略文档 | 2021 |
| 了解更多信息 | 2021 |
| AWSLambdaFullAccess | 2022 |
| 使用此策略 | 2022 |
| 策略详细信息 | 2022 |
| 策略版本 | 2022 |
| JSON 策略文档 | 2022 |
| 了解更多信息 | 2024 |
| AWSLambdaInvocation-DynamoDB | 2024 |
| 使用此策略 | 2024 |
| 策略详细信息 | 2024 |
| 策略版本 | 2024 |
| JSON 策略文档 | 2025 |
| 了解更多信息 | 2025 |
| AWSLambdaKinesisExecutionRole | 2025 |
| 使用此策略 | 2025 |
| 策略详细信息 | 2026 |
| 策略版本 | 2026 |
| JSON 策略文档 | 2026 |
| 了解更多信息 | 2027 |
| AWSLambdaMSKExecutionRole | 2027 |
| 使用此策略 | 2027 |
| 策略详细信息 | 2027 |
| 策略版本 | 2027 |
| JSON 策略文档 | 2027 |
| 了解更多信息 | 2028 |

| | |
|--|------|
| AWSLambdaReplicator | 2028 |
| 使用此策略 | 2028 |
| 策略详细信息 | 2028 |
| 策略版本 | 2029 |
| JSON 策略文档 | 2029 |
| 了解更多信息 | 2030 |
| AWSLambdaRole | 2030 |
| 使用此策略 | 2030 |
| 策略详细信息 | 2030 |
| 策略版本 | 2030 |
| JSON 策略文档 | 2031 |
| 了解更多信息 | 2031 |
| AWSLambdaSQSQueueExecutionRole | 2031 |
| 使用此策略 | 2031 |
| 策略详细信息 | 2031 |
| 策略版本 | 2032 |
| JSON 策略文档 | 2032 |
| 了解更多信息 | 2032 |
| AWSLambdaVPCLambdaAccessExecutionRole | 2033 |
| 使用此策略 | 2033 |
| 策略详细信息 | 2033 |
| 策略版本 | 2033 |
| JSON 策略文档 | 2033 |
| 了解更多信息 | 2034 |
| AWSLicenseManagerConsumptionPolicy | 2034 |
| 使用此策略 | 2034 |
| 策略详细信息 | 2034 |
| 策略版本 | 2034 |
| JSON 策略文档 | 2035 |
| 了解更多信息 | 2035 |
| AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy | 2035 |
| 使用此策略 | 2035 |
| 策略详细信息 | 2035 |
| 策略版本 | 2036 |
| JSON 策略文档 | 2036 |
| 了解更多信息 | 2037 |

| | |
|---|------|
| AWSLicenseManagerMasterAccountRolePolicy | 2037 |
| 使用此策略 | 2037 |
| 策略详细信息 | 2037 |
| 策略版本 | 2037 |
| JSON 策略文档 | 2038 |
| 了解更多信息 | 2042 |
| AWSLicenseManagerMemberAccountRolePolicy | 2043 |
| 使用此策略 | 2043 |
| 策略详细信息 | 2043 |
| 策略版本 | 2043 |
| JSON 策略文档 | 2043 |
| 了解更多信息 | 2044 |
| AWSLicenseManagerServiceRolePolicy | 2044 |
| 使用此策略 | 2045 |
| 策略详细信息 | 2045 |
| 策略版本 | 2045 |
| JSON 策略文档 | 2045 |
| 了解更多信息 | 2048 |
| AWSLicenseManagerUserSubscriptionsServiceRolePolicy | 2048 |
| 使用此策略 | 2049 |
| 策略详细信息 | 2049 |
| 策略版本 | 2049 |
| JSON 策略文档 | 2049 |
| 了解更多信息 | 2051 |
| AWSM2ServicePolicy | 2051 |
| 使用此策略 | 2051 |
| 策略详细信息 | 2051 |
| 策略版本 | 2052 |
| JSON 策略文档 | 2052 |
| 了解更多信息 | 2053 |
| AWSManagedServices_ContactsServiceRolePolicy | 2053 |
| 使用此策略 | 2053 |
| 策略详细信息 | 2053 |
| 策略版本 | 2054 |
| JSON 策略文档 | 2054 |
| 了解更多信息 | 2055 |

| | |
|--|------|
| AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy | 2055 |
| 使用此策略 | 2055 |
| 策略详细信息 | 2055 |
| 策略版本 | 2055 |
| JSON 策略文档 | 2055 |
| 了解更多信息 | 2057 |
| AWSManagedServices_EventsServiceRolePolicy | 2057 |
| 使用此策略 | 2057 |
| 策略详细信息 | 2057 |
| 策略版本 | 2057 |
| JSON 策略文档 | 2058 |
| 了解更多信息 | 2058 |
| AWSManagedServicesDeploymentToolkitPolicy | 2058 |
| 使用此策略 | 2059 |
| 策略详细信息 | 2059 |
| 策略版本 | 2059 |
| JSON 策略文档 | 2059 |
| 了解更多信息 | 2061 |
| AWSMarketplaceAmiIngestion | 2061 |
| 使用此策略 | 2061 |
| 策略详细信息 | 2061 |
| 策略版本 | 2062 |
| JSON 策略文档 | 2062 |
| 了解更多信息 | 2062 |
| AWSMarketplaceDeploymentServiceRolePolicy | 2063 |
| 使用此策略 | 2063 |
| 策略详细信息 | 2063 |
| 策略版本 | 2063 |
| JSON 策略文档 | 2063 |
| 了解更多信息 | 2065 |
| AWSMarketplaceFullAccess | 2065 |
| 使用此策略 | 2065 |
| 策略详细信息 | 2065 |
| 策略版本 | 2065 |
| JSON 策略文档 | 2065 |
| 了解更多信息 | 2068 |

| | |
|--|------|
| AWSMarketplaceGetEntitlements | 2069 |
| 使用此策略 | 2069 |
| 策略详细信息 | 2069 |
| 策略版本 | 2069 |
| JSON 策略文档 | 2069 |
| 了解更多信息 | 2070 |
| AWSMarketplaceImageBuildFullAccess | 2070 |
| 使用此策略 | 2070 |
| 策略详细信息 | 2070 |
| 策略版本 | 2070 |
| JSON 策略文档 | 2071 |
| 了解更多信息 | 2074 |
| AWSMarketplaceLicenseManagementServiceRolePolicy | 2074 |
| 使用此策略 | 2074 |
| 策略详细信息 | 2074 |
| 策略版本 | 2075 |
| JSON 策略文档 | 2075 |
| 了解更多信息 | 2075 |
| AWSMarketplaceManageSubscriptions | 2076 |
| 使用此策略 | 2076 |
| 策略详细信息 | 2076 |
| 策略版本 | 2076 |
| JSON 策略文档 | 2076 |
| 了解更多信息 | 2077 |
| AWSMarketplaceMeteringFullAccess | 2077 |
| 使用此策略 | 2077 |
| 策略详细信息 | 2077 |
| 策略版本 | 2078 |
| JSON 策略文档 | 2078 |
| 了解更多信息 | 2078 |
| AWSMarketplaceMeteringRegisterUsage | 2078 |
| 使用此策略 | 2079 |
| 策略详细信息 | 2079 |
| 策略版本 | 2079 |
| JSON 策略文档 | 2079 |
| 了解更多信息 | 2079 |

| | |
|--|------|
| AWSMarketplaceProcurementSystemAdminFullAccess | 2080 |
| 使用此策略 | 2080 |
| 策略详细信息 | 2080 |
| 策略版本 | 2080 |
| JSON 策略文档 | 2080 |
| 了解更多信息 | 2081 |
| AWSMarketplacePurchaseOrdersServiceRolePolicy | 2081 |
| 使用此策略 | 2081 |
| 策略详细信息 | 2081 |
| 策略版本 | 2081 |
| JSON 策略文档 | 2082 |
| 了解更多信息 | 2082 |
| AWSMarketplaceRead-only | 2082 |
| 使用此策略 | 2082 |
| 策略详细信息 | 2082 |
| 策略版本 | 2083 |
| JSON 策略文档 | 2083 |
| 了解更多信息 | 2084 |
| AWSMarketplaceResaleAuthorizationServiceRolePolicy | 2084 |
| 使用此策略 | 2084 |
| 策略详细信息 | 2084 |
| 策略版本 | 2085 |
| JSON 策略文档 | 2085 |
| 了解更多信息 | 2087 |
| AWSMarketplaceSellerFullAccess | 2087 |
| 使用此策略 | 2087 |
| 策略详细信息 | 2087 |
| 策略版本 | 2088 |
| JSON 策略文档 | 2088 |
| 了解更多信息 | 2091 |
| AWSMarketplaceSellerProductsFullAccess | 2091 |
| 使用此策略 | 2092 |
| 策略详细信息 | 2092 |
| 策略版本 | 2092 |
| JSON 策略文档 | 2092 |
| 了解更多信息 | 2094 |

| | |
|--|------|
| AWSMarketplaceSellerProductsReadOnly | 2094 |
| 使用此策略 | 2094 |
| 策略详细信息 | 2094 |
| 策略版本 | 2094 |
| JSON 策略文档 | 2095 |
| 了解更多信息 | 2095 |
| AWSMediaConnectServicePolicy | 2096 |
| 使用此策略 | 2096 |
| 策略详细信息 | 2096 |
| 策略版本 | 2096 |
| JSON 策略文档 | 2096 |
| 了解更多信息 | 2097 |
| AWSMediaTailorServiceRolePolicy | 2098 |
| 使用此策略 | 2098 |
| 策略详细信息 | 2098 |
| 策略版本 | 2098 |
| JSON 策略文档 | 2098 |
| 了解更多信息 | 2099 |
| AWSMigrationHubDiscoveryAccess | 2099 |
| 使用此策略 | 2099 |
| 策略详细信息 | 2099 |
| 策略版本 | 2099 |
| JSON 策略文档 | 2099 |
| 了解更多信息 | 2101 |
| AWSMigrationHubDMSAccess | 2101 |
| 使用此策略 | 2101 |
| 策略详细信息 | 2101 |
| 策略版本 | 2101 |
| JSON 策略文档 | 2102 |
| 了解更多信息 | 2103 |
| AWSMigrationHubFullAccess | 2103 |
| 使用此策略 | 2103 |
| 策略详细信息 | 2103 |
| 策略版本 | 2103 |
| JSON 策略文档 | 2103 |
| 了解更多信息 | 2105 |

| | |
|--|------|
| AWSMigrationHubOrchestratorConsoleFullAccess | 2105 |
| 使用此策略 | 2105 |
| 策略详细信息 | 2105 |
| 策略版本 | 2105 |
| JSON 策略文档 | 2106 |
| 了解更多信息 | 2109 |
| AWSMigrationHubOrchestratorInstanceRolePolicy | 2109 |
| 使用此策略 | 2109 |
| 策略详细信息 | 2109 |
| 策略版本 | 2109 |
| JSON 策略文档 | 2110 |
| 了解更多信息 | 2110 |
| AWSMigrationHubOrchestratorPlugin | 2110 |
| 使用此策略 | 2111 |
| 策略详细信息 | 2111 |
| 策略版本 | 2111 |
| JSON 策略文档 | 2111 |
| 了解更多信息 | 2112 |
| AWSMigrationHubOrchestratorServiceRolePolicy | 2113 |
| 使用此策略 | 2113 |
| 策略详细信息 | 2113 |
| 策略版本 | 2113 |
| JSON 策略文档 | 2113 |
| 了解更多信息 | 2117 |
| AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess | 2117 |
| 使用此策略 | 2117 |
| 策略详细信息 | 2117 |
| 策略版本 | 2117 |
| JSON 策略文档 | 2118 |
| 了解更多信息 | 2122 |
| AWSMigrationHubRefactorSpaces-SSMAutomationPolicy | 2123 |
| 使用此策略 | 2123 |
| 策略详细信息 | 2123 |
| 策略版本 | 2123 |
| JSON 策略文档 | 2123 |
| 了解更多信息 | 2125 |

| | |
|--|------|
| AWSMigrationHubRefactorSpacesFullAccess | 2125 |
| 使用此策略 | 2125 |
| 策略详细信息 | 2125 |
| 策略版本 | 2125 |
| JSON 策略文档 | 2126 |
| 了解更多信息 | 2131 |
| AWSMigrationHubRefactorSpacesServiceRolePolicy | 2132 |
| 使用此策略 | 2132 |
| 策略详细信息 | 2132 |
| 策略版本 | 2132 |
| JSON 策略文档 | 2132 |
| 了解更多信息 | 2136 |
| AWSMigrationHubSMSAccess | 2136 |
| 使用此策略 | 2136 |
| 策略详细信息 | 2136 |
| 策略版本 | 2136 |
| JSON 策略文档 | 2137 |
| 了解更多信息 | 2138 |
| AWSMigrationHubStrategyCollector | 2138 |
| 使用此策略 | 2138 |
| 策略详细信息 | 2138 |
| 策略版本 | 2138 |
| JSON 策略文档 | 2138 |
| 了解更多信息 | 2140 |
| AWSMigrationHubStrategyConsoleFullAccess | 2141 |
| 使用此策略 | 2141 |
| 策略详细信息 | 2141 |
| 策略版本 | 2141 |
| JSON 策略文档 | 2141 |
| 了解更多信息 | 2143 |
| AWSMigrationHubStrategyServiceRolePolicy | 2143 |
| 使用此策略 | 2143 |
| 策略详细信息 | 2143 |
| 策略版本 | 2144 |
| JSON 策略文档 | 2144 |
| 了解更多信息 | 2145 |

| | |
|--|------|
| AWSMobileHub_FullAccess | 2145 |
| 使用此策略 | 2145 |
| 策略详细信息 | 2145 |
| 策略版本 | 2145 |
| JSON 策略文档 | 2146 |
| 了解更多信息 | 2147 |
| AWSMobileHub_ReadOnly | 2147 |
| 使用此策略 | 2147 |
| 策略详细信息 | 2147 |
| 策略版本 | 2148 |
| JSON 策略文档 | 2148 |
| 了解更多信息 | 2149 |
| AWSMSKReplicatorExecutionRole | 2149 |
| 使用此策略 | 2149 |
| 策略详细信息 | 2149 |
| 策略版本 | 2150 |
| JSON 策略文档 | 2150 |
| 了解更多信息 | 2151 |
| AWSNetworkFirewallServiceRolePolicy | 2151 |
| 使用此策略 | 2151 |
| 策略详细信息 | 2152 |
| 策略版本 | 2152 |
| JSON 策略文档 | 2152 |
| 了解更多信息 | 2153 |
| AWSNetworkManagerCloudWANServiceRolePolicy | 2154 |
| 使用此策略 | 2154 |
| 策略详细信息 | 2154 |
| 策略版本 | 2154 |
| JSON 策略文档 | 2154 |
| 了解更多信息 | 2155 |
| AWSNetworkManagerFullAccess | 2155 |
| 使用此策略 | 2155 |
| 策略详细信息 | 2155 |
| 策略版本 | 2155 |
| JSON 策略文档 | 2155 |
| 了解更多信息 | 2156 |

| | |
|--|------|
| AWSNetworkManagerReadOnlyAccess | 2156 |
| 使用此策略 | 2156 |
| 策略详细信息 | 2156 |
| 策略版本 | 2157 |
| JSON 策略文档 | 2157 |
| 了解更多信息 | 2157 |
| AWSNetworkManagerServiceRolePolicy | 2157 |
| 使用此策略 | 2158 |
| 策略详细信息 | 2158 |
| 策略版本 | 2158 |
| JSON 策略文档 | 2158 |
| 了解更多信息 | 2159 |
| AWSOpsWorks_FullAccess | 2159 |
| 使用此策略 | 2159 |
| 策略详细信息 | 2159 |
| 策略版本 | 2160 |
| JSON 策略文档 | 2160 |
| 了解更多信息 | 2161 |
| AWSOpsWorksCloudWatchLogs | 2161 |
| 使用此策略 | 2161 |
| 策略详细信息 | 2161 |
| 策略版本 | 2161 |
| JSON 策略文档 | 2162 |
| 了解更多信息 | 2162 |
| AWSOpsWorksCMInstanceProfileRole | 2162 |
| 使用此策略 | 2162 |
| 策略详细信息 | 2162 |
| 策略版本 | 2163 |
| JSON 策略文档 | 2163 |
| 了解更多信息 | 2164 |
| AWSOpsWorksCMServiceRole | 2164 |
| 使用此策略 | 2164 |
| 策略详细信息 | 2164 |
| 策略版本 | 2164 |
| JSON 策略文档 | 2165 |
| 了解更多信息 | 2169 |

| | |
|--|------|
| AWSOpsWorksInstanceRegistration | 2169 |
| 使用此策略 | 2169 |
| 策略详细信息 | 2169 |
| 策略版本 | 2169 |
| JSON 策略文档 | 2170 |
| 了解更多信息 | 2170 |
| AWSOpsWorksRegisterCLI_EC2 | 2170 |
| 使用此策略 | 2170 |
| 策略详细信息 | 2170 |
| 策略版本 | 2171 |
| JSON 策略文档 | 2171 |
| 了解更多信息 | 2172 |
| AWSOpsWorksRegisterCLI_OnPremises | 2172 |
| 使用此策略 | 2172 |
| 策略详细信息 | 2172 |
| 策略版本 | 2172 |
| JSON 策略文档 | 2172 |
| 了解更多信息 | 2174 |
| AWSOrganizationsFullAccess | 2174 |
| 使用此策略 | 2174 |
| 策略详细信息 | 2174 |
| 策略版本 | 2175 |
| JSON 策略文档 | 2175 |
| 了解更多信息 | 2176 |
| AWSOrganizationsReadOnlyAccess | 2176 |
| 使用此策略 | 2176 |
| 策略详细信息 | 2176 |
| 策略版本 | 2176 |
| JSON 策略文档 | 2176 |
| 了解更多信息 | 2177 |
| AWSOrganizationsServiceTrustPolicy | 2177 |
| 使用此策略 | 2177 |
| 策略详细信息 | 2178 |
| 策略版本 | 2178 |
| JSON 策略文档 | 2178 |
| 了解更多信息 | 2179 |

| | |
|---|------|
| AWSOutpostsAuthorizeServerPolicy | 2179 |
| 使用此策略 | 2179 |
| 策略详细信息 | 2179 |
| 策略版本 | 2179 |
| JSON 策略文档 | 2179 |
| 了解更多信息 | 2180 |
| AWSOutpostsServiceRolePolicy | 2180 |
| 使用此策略 | 2180 |
| 策略详细信息 | 2180 |
| 策略版本 | 2180 |
| JSON 策略文档 | 2181 |
| 了解更多信息 | 2181 |
| AWSPanoramaApplianceRolePolicy | 2181 |
| 使用此策略 | 2181 |
| 策略详细信息 | 2181 |
| 策略版本 | 2182 |
| JSON 策略文档 | 2182 |
| 了解更多信息 | 2182 |
| AWSPanoramaApplianceServiceRolePolicy | 2183 |
| 使用此策略 | 2183 |
| 策略详细信息 | 2183 |
| 策略版本 | 2183 |
| JSON 策略文档 | 2183 |
| 了解更多信息 | 2185 |
| AWSPanoramaFullAccess | 2185 |
| 使用此策略 | 2185 |
| 策略详细信息 | 2185 |
| 策略版本 | 2185 |
| JSON 策略文档 | 2185 |
| 了解更多信息 | 2188 |
| AWSPanoramaGreengrassGroupRolePolicy | 2188 |
| 使用此策略 | 2188 |
| 策略详细信息 | 2188 |
| 策略版本 | 2189 |
| JSON 策略文档 | 2189 |
| 了解更多信息 | 2190 |

| | |
|--|------|
| AWSPanoramaSageMakerRolePolicy | 2190 |
| 使用此策略 | 2190 |
| 策略详细信息 | 2190 |
| 策略版本 | 2191 |
| JSON 策略文档 | 2191 |
| 了解更多信息 | 2191 |
| AWSPanoramaServiceLinkedRolePolicy | 2192 |
| 使用此策略 | 2192 |
| 策略详细信息 | 2192 |
| 策略版本 | 2192 |
| JSON 策略文档 | 2192 |
| 了解更多信息 | 2195 |
| AWSPanoramaServiceRolePolicy | 2195 |
| 使用此策略 | 2195 |
| 策略详细信息 | 2195 |
| 策略版本 | 2195 |
| JSON 策略文档 | 2196 |
| 了解更多信息 | 2202 |
| AWSPriceListServiceFullAccess | 2203 |
| 使用此策略 | 2203 |
| 策略详细信息 | 2203 |
| 策略版本 | 2203 |
| JSON 策略文档 | 2203 |
| 了解更多信息 | 2204 |
| AWSPrivateCAAuditor | 2204 |
| 使用此策略 | 2204 |
| 策略详细信息 | 2204 |
| 策略版本 | 2204 |
| JSON 策略文档 | 2204 |
| 了解更多信息 | 2205 |
| AWSPrivateCAFullAccess | 2205 |
| 使用此策略 | 2205 |
| 策略详细信息 | 2206 |
| 策略版本 | 2206 |
| JSON 策略文档 | 2206 |
| 了解更多信息 | 2206 |

| | |
|---|------|
| AWSPriateCAPrivilegedUser | 2207 |
| 使用此策略 | 2207 |
| 策略详细信息 | 2207 |
| 策略版本 | 2207 |
| JSON 策略文档 | 2207 |
| 了解更多信息 | 2208 |
| AWSPriateCARedOnly | 2209 |
| 使用此策略 | 2209 |
| 策略详细信息 | 2209 |
| 策略版本 | 2209 |
| JSON 策略文档 | 2209 |
| 了解更多信息 | 2210 |
| AWSPriateCAUser | 2210 |
| 使用此策略 | 2210 |
| 策略详细信息 | 2210 |
| 策略版本 | 2210 |
| JSON 策略文档 | 2211 |
| 了解更多信息 | 2212 |
| AWSPriateMarketplaceAdminFullAccess | 2212 |
| 使用此策略 | 2212 |
| 策略详细信息 | 2212 |
| 策略版本 | 2212 |
| JSON 策略文档 | 2213 |
| 了解更多信息 | 2214 |
| AWSPriateMarketplaceRequests | 2214 |
| 使用此策略 | 2214 |
| 策略详细信息 | 2214 |
| 策略版本 | 2215 |
| JSON 策略文档 | 2215 |
| 了解更多信息 | 2215 |
| AWSPriateNetworksServiceRolePolicy | 2215 |
| 使用此策略 | 2216 |
| 策略详细信息 | 2216 |
| 策略版本 | 2216 |
| JSON 策略文档 | 2216 |
| 了解更多信息 | 2217 |

| | |
|---|------|
| AWSProtonCodeBuildProvisioningBasicAccess | 2217 |
| 使用此策略 | 2217 |
| 策略详细信息 | 2217 |
| 策略版本 | 2217 |
| JSON 策略文档 | 2217 |
| 了解更多信息 | 2218 |
| AWSProtonCodeBuildProvisioningServiceRolePolicy | 2218 |
| 使用此策略 | 2218 |
| 策略详细信息 | 2218 |
| 策略版本 | 2219 |
| JSON 策略文档 | 2219 |
| 了解更多信息 | 2220 |
| AWSProtonDeveloperAccess | 2220 |
| 使用此策略 | 2220 |
| 策略详细信息 | 2220 |
| 策略版本 | 2221 |
| JSON 策略文档 | 2221 |
| 了解更多信息 | 2223 |
| AWSProtonFullAccess | 2223 |
| 使用此策略 | 2223 |
| 策略详细信息 | 2223 |
| 策略版本 | 2223 |
| JSON 策略文档 | 2223 |
| 了解更多信息 | 2225 |
| AWSProtonReadOnlyAccess | 2225 |
| 使用此策略 | 2225 |
| 策略详细信息 | 2225 |
| 策略版本 | 2226 |
| JSON 策略文档 | 2226 |
| 了解更多信息 | 2227 |
| AWSProtonServiceGitSyncServiceRolePolicy | 2227 |
| 使用此策略 | 2227 |
| 策略详细信息 | 2228 |
| 策略版本 | 2228 |
| JSON 策略文档 | 2228 |
| 了解更多信息 | 2229 |

| | |
|--|------|
| AWSProtonSyncServiceRolePolicy | 2229 |
| 使用此策略 | 2229 |
| 策略详细信息 | 2229 |
| 策略版本 | 2229 |
| JSON 策略文档 | 2229 |
| 了解更多信息 | 2230 |
| AWSPurchaseOrdersServiceRolePolicy | 2231 |
| 使用此策略 | 2231 |
| 策略详细信息 | 2231 |
| 策略版本 | 2231 |
| JSON 策略文档 | 2231 |
| 了解更多信息 | 2232 |
| AWSQuicksightAthenaAccess | 2232 |
| 使用此策略 | 2232 |
| 策略详细信息 | 2232 |
| 策略版本 | 2233 |
| JSON 策略文档 | 2233 |
| 了解更多信息 | 2235 |
| AWSQuickSightDescribeRDS | 2235 |
| 使用此策略 | 2235 |
| 策略详细信息 | 2235 |
| 策略版本 | 2236 |
| JSON 策略文档 | 2236 |
| 了解更多信息 | 2236 |
| AWSQuickSightDescribeRedshift | 2236 |
| 使用此策略 | 2236 |
| 策略详细信息 | 2237 |
| 策略版本 | 2237 |
| JSON 策略文档 | 2237 |
| 了解更多信息 | 2237 |
| AWSQuickSightElasticsearchPolicy | 2238 |
| 使用此策略 | 2238 |
| 策略详细信息 | 2238 |
| 策略版本 | 2238 |
| JSON 策略文档 | 2238 |
| 了解更多信息 | 2239 |

| | |
|--|------|
| AWSQuickSightIoTAnalyticsAccess | 2239 |
| 使用此策略 | 2240 |
| 策略详细信息 | 2240 |
| 策略版本 | 2240 |
| JSON 策略文档 | 2240 |
| 了解更多信息 | 2240 |
| AWSQuickSightListIAM | 2241 |
| 使用此策略 | 2241 |
| 策略详细信息 | 2241 |
| 策略版本 | 2241 |
| JSON 策略文档 | 2241 |
| 了解更多信息 | 2242 |
| AWSQuickSightOpenSearchPolicy | 2242 |
| 使用此策略 | 2242 |
| 策略详细信息 | 2242 |
| 策略版本 | 2242 |
| JSON 策略文档 | 2242 |
| 了解更多信息 | 2243 |
| AWSQuickSightSageMakerPolicy | 2244 |
| 使用此策略 | 2244 |
| 策略详细信息 | 2244 |
| 策略版本 | 2244 |
| JSON 策略文档 | 2244 |
| 了解更多信息 | 2245 |
| AWSQuickSightTimestreamPolicy | 2246 |
| 使用此策略 | 2246 |
| 策略详细信息 | 2246 |
| 策略版本 | 2246 |
| JSON 策略文档 | 2246 |
| 了解更多信息 | 2247 |
| AWSReachabilityAnalyzerServiceRolePolicy | 2247 |
| 使用此策略 | 2247 |
| 策略详细信息 | 2247 |
| 策略版本 | 2248 |
| JSON 策略文档 | 2248 |
| 了解更多信息 | 2250 |

| | |
|---|------|
| AWSRefactoringToolkitFullAccess | 2250 |
| 使用此策略 | 2250 |
| 策略详细信息 | 2250 |
| 策略版本 | 2251 |
| JSON 策略文档 | 2251 |
| 了解更多信息 | 2264 |
| AWSRefactoringToolkitSidecarPolicy | 2264 |
| 使用此策略 | 2265 |
| 策略详细信息 | 2265 |
| 策略版本 | 2265 |
| JSON 策略文档 | 2265 |
| 了解更多信息 | 2266 |
| AWSrePostPrivateCloudWatchAccess | 2266 |
| 使用此策略 | 2266 |
| 策略详细信息 | 2266 |
| 策略版本 | 2267 |
| JSON 策略文档 | 2267 |
| 了解更多信息 | 2267 |
| AWSRepostSpaceSupportOperationsPolicy | 2268 |
| 使用此策略 | 2268 |
| 策略详细信息 | 2268 |
| 策略版本 | 2268 |
| JSON 策略文档 | 2268 |
| 了解更多信息 | 2269 |
| AWSResilienceHubAssessmentExecutionPolicy | 2269 |
| 使用此策略 | 2269 |
| 策略详细信息 | 2269 |
| 策略版本 | 2269 |
| JSON 策略文档 | 2270 |
| 了解更多信息 | 2273 |
| AWSResourceAccessManagerFullAccess | 2274 |
| 使用此策略 | 2274 |
| 策略详细信息 | 2274 |
| 策略版本 | 2274 |
| JSON 策略文档 | 2274 |
| 了解更多信息 | 2275 |

| | |
|--|------|
| AWSResourceAccessManagerReadOnlyAccess | 2275 |
| 使用此策略 | 2275 |
| 策略详细信息 | 2275 |
| 策略版本 | 2275 |
| JSON 策略文档 | 2275 |
| 了解更多信息 | 2276 |
| AWSResourceAccessManagerResourceShareParticipantAccess | 2276 |
| 使用此策略 | 2276 |
| 策略详细信息 | 2276 |
| 策略版本 | 2277 |
| JSON 策略文档 | 2277 |
| 了解更多信息 | 2277 |
| AWSResourceAccessManagerServiceRolePolicy | 2278 |
| 使用此策略 | 2278 |
| 策略详细信息 | 2278 |
| 策略版本 | 2278 |
| JSON 策略文档 | 2278 |
| 了解更多信息 | 2279 |
| AWSResourceExplorerFullAccess | 2279 |
| 使用此策略 | 2279 |
| 策略详细信息 | 2279 |
| 策略版本 | 2280 |
| JSON 策略文档 | 2280 |
| 了解更多信息 | 2281 |
| AWSResourceExplorerOrganizationsAccess | 2281 |
| 使用此策略 | 2281 |
| 策略详细信息 | 2281 |
| 策略版本 | 2281 |
| JSON 策略文档 | 2281 |
| 了解更多信息 | 2283 |
| AWSResourceExplorerReadOnlyAccess | 2283 |
| 使用此策略 | 2283 |
| 策略详细信息 | 2283 |
| 策略版本 | 2284 |
| JSON 策略文档 | 2284 |
| 了解更多信息 | 2284 |

| | |
|--|------|
| AWSResourceExplorerServiceRolePolicy | 2285 |
| 使用此策略 | 2285 |
| 策略详细信息 | 2285 |
| 策略版本 | 2285 |
| JSON 策略文档 | 2285 |
| 了解更多信息 | 2294 |
| AWSResourceGroupsReadOnlyAccess | 2294 |
| 使用此策略 | 2295 |
| 策略详细信息 | 2295 |
| 策略版本 | 2295 |
| JSON 策略文档 | 2295 |
| 了解更多信息 | 2296 |
| AWSRoboMaker_FullAccess | 2297 |
| 使用此策略 | 2297 |
| 策略详细信息 | 2297 |
| 策略版本 | 2297 |
| JSON 策略文档 | 2297 |
| 了解更多信息 | 2298 |
| AWSRoboMakerReadOnlyAccess | 2299 |
| 使用此策略 | 2299 |
| 策略详细信息 | 2299 |
| 策略版本 | 2299 |
| JSON 策略文档 | 2299 |
| 了解更多信息 | 2300 |
| AWSRoboMakerServicePolicy | 2300 |
| 使用此策略 | 2300 |
| 策略详细信息 | 2300 |
| 策略版本 | 2300 |
| JSON 策略文档 | 2300 |
| 了解更多信息 | 2302 |
| AWSRoboMakerServiceRolePolicy | 2302 |
| 使用此策略 | 2302 |
| 策略详细信息 | 2302 |
| 策略版本 | 2303 |
| JSON 策略文档 | 2303 |
| 了解更多信息 | 2304 |

| | |
|---|------|
| AWSRolesAnywhereServicePolicy | 2304 |
| 使用此策略 | 2304 |
| 策略详细信息 | 2304 |
| 策略版本 | 2305 |
| JSON 策略文档 | 2305 |
| 了解更多信息 | 2305 |
| AWSS3OnOutpostsServiceRolePolicy | 2306 |
| 使用此策略 | 2306 |
| 策略详细信息 | 2306 |
| 策略版本 | 2306 |
| JSON 策略文档 | 2306 |
| 了解更多信息 | 2309 |
| AWSSavingsPlansFullAccess | 2309 |
| 使用此策略 | 2309 |
| 策略详细信息 | 2309 |
| 策略版本 | 2309 |
| JSON 策略文档 | 2309 |
| 了解更多信息 | 2310 |
| AWSSavingsPlansReadOnlyAccess | 2310 |
| 使用此策略 | 2310 |
| 策略详细信息 | 2310 |
| 策略版本 | 2310 |
| JSON 策略文档 | 2311 |
| 了解更多信息 | 2311 |
| AWSSecurityHubFullAccess | 2311 |
| 使用此策略 | 2311 |
| 策略详细信息 | 2311 |
| 策略版本 | 2312 |
| JSON 策略文档 | 2312 |
| 了解更多信息 | 2313 |
| AWSSecurityHubOrganizationsAccess | 2313 |
| 使用此策略 | 2313 |
| 策略详细信息 | 2313 |
| 策略版本 | 2313 |
| JSON 策略文档 | 2313 |
| 了解更多信息 | 2315 |

| | |
|--|------|
| AWSSecurityHubReadOnlyAccess | 2315 |
| 使用此策略 | 2315 |
| 策略详细信息 | 2315 |
| 策略版本 | 2315 |
| JSON 策略文档 | 2315 |
| 了解更多信息 | 2316 |
| AWSSecurityHubServiceRolePolicy | 2316 |
| 使用此策略 | 2316 |
| 策略详细信息 | 2316 |
| 策略版本 | 2317 |
| JSON 策略文档 | 2317 |
| 了解更多信息 | 2319 |
| AWSServiceCatalogAdminFullAccess | 2319 |
| 使用此策略 | 2319 |
| 策略详细信息 | 2319 |
| 策略版本 | 2319 |
| JSON 策略文档 | 2319 |
| 了解更多信息 | 2322 |
| AWSServiceCatalogAdminReadOnlyAccess | 2322 |
| 使用此策略 | 2322 |
| 策略详细信息 | 2323 |
| 策略版本 | 2323 |
| JSON 策略文档 | 2323 |
| 了解更多信息 | 2324 |
| AWSServiceCatalogAppRegistryFullAccess | 2324 |
| 使用此策略 | 2325 |
| 策略详细信息 | 2325 |
| 策略版本 | 2325 |
| JSON 策略文档 | 2325 |
| 了解更多信息 | 2327 |
| AWSServiceCatalogAppRegistryReadOnlyAccess | 2327 |
| 使用此策略 | 2328 |
| 策略详细信息 | 2328 |
| 策略版本 | 2328 |
| JSON 策略文档 | 2328 |
| 了解更多信息 | 2329 |

| | |
|--|------|
| AWSServiceCatalogAppRegistryServiceRolePolicy | 2329 |
| 使用此策略 | 2329 |
| 策略详细信息 | 2329 |
| 策略版本 | 2329 |
| JSON 策略文档 | 2329 |
| 了解更多信息 | 2331 |
| AWSServiceCatalogEndUserFullAccess | 2331 |
| 使用此策略 | 2331 |
| 策略详细信息 | 2331 |
| 策略版本 | 2331 |
| JSON 策略文档 | 2331 |
| 了解更多信息 | 2333 |
| AWSServiceCatalogEndUserReadOnlyAccess | 2334 |
| 使用此策略 | 2334 |
| 策略详细信息 | 2334 |
| 策略版本 | 2334 |
| JSON 策略文档 | 2334 |
| 了解更多信息 | 2336 |
| AWSServiceCatalogOrgsDataSyncServiceRolePolicy | 2336 |
| 使用此策略 | 2336 |
| 策略详细信息 | 2336 |
| 策略版本 | 2337 |
| JSON 策略文档 | 2337 |
| 了解更多信息 | 2337 |
| AWSServiceCatalogSyncServiceRolePolicy | 2337 |
| 使用此策略 | 2338 |
| 策略详细信息 | 2338 |
| 策略版本 | 2338 |
| JSON 策略文档 | 2338 |
| 了解更多信息 | 2339 |
| AWSServiceRoleForAmazonEKSNodegroup | 2339 |
| 使用此策略 | 2339 |
| 策略详细信息 | 2339 |
| 策略版本 | 2340 |
| JSON 策略文档 | 2340 |
| 了解更多信息 | 2344 |

| | |
|--|------|
| AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy | 2344 |
| 使用此策略 | 2344 |
| 策略详细信息 | 2344 |
| 策略版本 | 2344 |
| JSON 策略文档 | 2345 |
| 了解更多信息 | 2345 |
| AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy | 2345 |
| 使用此策略 | 2345 |
| 策略详细信息 | 2345 |
| 策略版本 | 2346 |
| JSON 策略文档 | 2346 |
| 了解更多信息 | 2346 |
| AWSServiceRoleForCodeGuru-Profiler | 2346 |
| 使用此策略 | 2346 |
| 策略详细信息 | 2347 |
| 策略版本 | 2347 |
| JSON 策略文档 | 2347 |
| 了解更多信息 | 2347 |
| AWSServiceRoleForCodeWhispererPolicy | 2348 |
| 使用此策略 | 2348 |
| 策略详细信息 | 2348 |
| 策略版本 | 2348 |
| JSON 策略文档 | 2348 |
| 了解更多信息 | 2350 |
| AWSServiceRoleForEC2ScheduledInstances | 2350 |
| 使用此策略 | 2350 |
| 策略详细信息 | 2350 |
| 策略版本 | 2351 |
| JSON 策略文档 | 2351 |
| 了解更多信息 | 2352 |
| AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy | 2352 |
| 使用此策略 | 2352 |
| 策略详细信息 | 2352 |
| 策略版本 | 2352 |
| JSON 策略文档 | 2352 |
| 了解更多信息 | 2353 |

| | |
|--|------|
| AWSServiceRoleForImageBuilder | 2353 |
| 使用此策略 | 2353 |
| 策略详细信息 | 2353 |
| 策略版本 | 2353 |
| JSON 策略文档 | 2354 |
| 了解更多信息 | 2363 |
| AWSServiceRoleForIoTSiteWise | 2363 |
| 使用此策略 | 2363 |
| 策略详细信息 | 2364 |
| 策略版本 | 2364 |
| JSON 策略文档 | 2364 |
| 了解更多信息 | 2365 |
| AWSServiceRoleForLogDeliveryPolicy | 2365 |
| 使用此策略 | 2366 |
| 策略详细信息 | 2366 |
| 策略版本 | 2366 |
| JSON 策略文档 | 2366 |
| 了解更多信息 | 2367 |
| AWSServiceRoleForMonitronPolicy | 2367 |
| 使用此策略 | 2367 |
| 策略详细信息 | 2367 |
| 策略版本 | 2367 |
| JSON 策略文档 | 2367 |
| 了解更多信息 | 2368 |
| AWSServiceRoleForNeptuneGraphPolicy | 2368 |
| 使用此策略 | 2368 |
| 策略详细信息 | 2368 |
| 策略版本 | 2369 |
| JSON 策略文档 | 2369 |
| 了解更多信息 | 2370 |
| AWSServiceRoleForPrivateMarketplaceAdminPolicy | 2370 |
| 使用此策略 | 2370 |
| 策略详细信息 | 2370 |
| 策略版本 | 2371 |
| JSON 策略文档 | 2371 |
| 了解更多信息 | 2372 |

| | |
|---|------|
| AWSServiceRoleForSMS | 2373 |
| 使用此策略 | 2373 |
| 策略详细信息 | 2373 |
| 策略版本 | 2373 |
| JSON 策略文档 | 2373 |
| 了解更多信息 | 2380 |
| AWSServiceRolePolicyForBackupReports | 2380 |
| 使用此策略 | 2380 |
| 策略详细信息 | 2380 |
| 策略版本 | 2380 |
| JSON 策略文档 | 2381 |
| 了解更多信息 | 2382 |
| AWSServiceRolePolicyForBackupRestoreTesting | 2382 |
| 使用此策略 | 2382 |
| 策略详细信息 | 2382 |
| 策略版本 | 2382 |
| JSON 策略文档 | 2383 |
| 了解更多信息 | 2385 |
| AWSShieldDRTAcessPolicy | 2386 |
| 使用此策略 | 2386 |
| 策略详细信息 | 2386 |
| 策略版本 | 2386 |
| JSON 策略文档 | 2386 |
| 了解更多信息 | 2387 |
| AWSShieldServiceRolePolicy | 2387 |
| 使用此策略 | 2387 |
| 策略详细信息 | 2388 |
| 策略版本 | 2388 |
| JSON 策略文档 | 2388 |
| 了解更多信息 | 2388 |
| AWSSSMForSAPServiceLinkedRolePolicy | 2389 |
| 使用此策略 | 2389 |
| 策略详细信息 | 2389 |
| 策略版本 | 2389 |
| JSON 策略文档 | 2389 |
| 了解更多信息 | 2395 |

| | |
|--|------|
| AWSSSMOpsInsightsServiceRolePolicy | 2395 |
| 使用此策略 | 2396 |
| 策略详细信息 | 2396 |
| 策略版本 | 2396 |
| JSON 策略文档 | 2396 |
| 了解更多信息 | 2397 |
| AWSSSODirectoryAdministrator | 2397 |
| 使用此策略 | 2397 |
| 策略详细信息 | 2397 |
| 策略版本 | 2397 |
| JSON 策略文档 | 2398 |
| 了解更多信息 | 2398 |
| AWSSSODirectoryReadOnly | 2398 |
| 使用此策略 | 2398 |
| 策略详细信息 | 2398 |
| 策略版本 | 2399 |
| JSON 策略文档 | 2399 |
| 了解更多信息 | 2399 |
| AWSSSOMasterAccountAdministrator | 2400 |
| 使用此策略 | 2400 |
| 策略详细信息 | 2400 |
| 策略版本 | 2400 |
| JSON 策略文档 | 2400 |
| 了解更多信息 | 2402 |
| AWSSSOMemberAccountAdministrator | 2402 |
| 使用此策略 | 2402 |
| 策略详细信息 | 2402 |
| 策略版本 | 2403 |
| JSON 策略文档 | 2403 |
| 了解更多信息 | 2404 |
| AWSSSOReadOnly | 2404 |
| 使用此策略 | 2404 |
| 策略详细信息 | 2404 |
| 策略版本 | 2405 |
| JSON 策略文档 | 2405 |
| 了解更多信息 | 2406 |

| | |
|--|------|
| AWSSSOServiceRolePolicy | 2406 |
| 使用此策略 | 2406 |
| 策略详细信息 | 2406 |
| 策略版本 | 2406 |
| JSON 策略文档 | 2406 |
| 了解更多信息 | 2410 |
| AWSSStepFunctionsConsoleFullAccess | 2410 |
| 使用此策略 | 2410 |
| 策略详细信息 | 2410 |
| 策略版本 | 2410 |
| JSON 策略文档 | 2411 |
| 了解更多信息 | 2411 |
| AWSSStepFunctionsFullAccess | 2412 |
| 使用此策略 | 2412 |
| 策略详细信息 | 2412 |
| 策略版本 | 2412 |
| JSON 策略文档 | 2412 |
| 了解更多信息 | 2413 |
| AWSSStepFunctionsReadOnlyAccess | 2413 |
| 使用此策略 | 2413 |
| 策略详细信息 | 2413 |
| 策略版本 | 2413 |
| JSON 策略文档 | 2413 |
| 了解更多信息 | 2414 |
| AWSSStorageGatewayFullAccess | 2414 |
| 使用此策略 | 2414 |
| 策略详细信息 | 2414 |
| 策略版本 | 2415 |
| JSON 策略文档 | 2415 |
| 了解更多信息 | 2415 |
| AWSSStorageGatewayReadOnlyAccess | 2416 |
| 使用此策略 | 2416 |
| 策略详细信息 | 2416 |
| 策略版本 | 2416 |
| JSON 策略文档 | 2416 |
| 了解更多信息 | 2417 |

| | |
|---|------|
| AWSStrorageGatewayServiceRolePolicy | 2417 |
| 使用此策略 | 2417 |
| 策略详细信息 | 2417 |
| 策略版本 | 2418 |
| JSON 策略文档 | 2418 |
| 了解更多信息 | 2418 |
| AWSSupplyChainFederationAdminAccess | 2418 |
| 使用此策略 | 2418 |
| 策略详细信息 | 2419 |
| 策略版本 | 2419 |
| JSON 策略文档 | 2419 |
| 了解更多信息 | 2424 |
| AWSSupportAccess | 2424 |
| 使用此策略 | 2425 |
| 策略详细信息 | 2425 |
| 策略版本 | 2425 |
| JSON 策略文档 | 2425 |
| 了解更多信息 | 2425 |
| AWSSupportAppFullAccess | 2426 |
| 使用此策略 | 2426 |
| 策略详细信息 | 2426 |
| 策略版本 | 2426 |
| JSON 策略文档 | 2426 |
| 了解更多信息 | 2427 |
| AWSSupportAppReadOnlyAccess | 2427 |
| 使用此策略 | 2427 |
| 策略详细信息 | 2428 |
| 策略版本 | 2428 |
| JSON 策略文档 | 2428 |
| 了解更多信息 | 2428 |
| AWSSupportPlansFullAccess | 2429 |
| 使用此策略 | 2429 |
| 策略详细信息 | 2429 |
| 策略版本 | 2429 |
| JSON 策略文档 | 2429 |
| 了解更多信息 | 2430 |

| | |
|--|------|
| AWSSupportPlansReadOnlyAccess | 2430 |
| 使用此策略 | 2430 |
| 策略详细信息 | 2430 |
| 策略版本 | 2430 |
| JSON 策略文档 | 2430 |
| 了解更多信息 | 2431 |
| AWSSupportServiceRolePolicy | 2431 |
| 使用此策略 | 2431 |
| 策略详细信息 | 2431 |
| 策略版本 | 2431 |
| JSON 策略文档 | 2432 |
| 了解更多信息 | 2505 |
| AWSSystemsManagerAccountDiscoveryServicePolicy | 2505 |
| 使用此策略 | 2506 |
| 策略详细信息 | 2506 |
| 策略版本 | 2506 |
| JSON 策略文档 | 2506 |
| 了解更多信息 | 2507 |
| AWSSystemsManagerChangeManagementServicePolicy | 2507 |
| 使用此策略 | 2507 |
| 策略详细信息 | 2507 |
| 策略版本 | 2507 |
| JSON 策略文档 | 2507 |
| 了解更多信息 | 2509 |
| AWSSystemsManagerForSAPFullAccess | 2509 |
| 使用此策略 | 2509 |
| 策略详细信息 | 2509 |
| 策略版本 | 2510 |
| JSON 策略文档 | 2510 |
| 了解更多信息 | 2511 |
| AWSSystemsManagerForSAPReadOnlyAccess | 2511 |
| 使用此策略 | 2511 |
| 策略详细信息 | 2511 |
| 策略版本 | 2511 |
| JSON 策略文档 | 2511 |
| 了解更多信息 | 2512 |

| | |
|--|------|
| AWSSystemsManagerOpsDataSyncServiceRolePolicy | 2512 |
| 使用此策略 | 2512 |
| 策略详细信息 | 2512 |
| 策略版本 | 2512 |
| JSON 策略文档 | 2513 |
| 了解更多信息 | 2516 |
| AWSThinkboxAssetServerPolicy | 2516 |
| 使用此策略 | 2516 |
| 策略详细信息 | 2517 |
| 策略版本 | 2517 |
| JSON 策略文档 | 2517 |
| 了解更多信息 | 2518 |
| AWSThinkboxAWSPortalAdminPolicy | 2518 |
| 使用此策略 | 2518 |
| 策略详细信息 | 2518 |
| 策略版本 | 2518 |
| JSON 策略文档 | 2518 |
| 了解更多信息 | 2528 |
| AWSThinkboxAWSPortalGatewayPolicy | 2528 |
| 使用此策略 | 2529 |
| 策略详细信息 | 2529 |
| 策略版本 | 2529 |
| JSON 策略文档 | 2529 |
| 了解更多信息 | 2531 |
| AWSThinkboxAWSPortalWorkerPolicy | 2531 |
| 使用此策略 | 2531 |
| 策略详细信息 | 2531 |
| 策略版本 | 2531 |
| JSON 策略文档 | 2532 |
| 了解更多信息 | 2533 |
| AWSThinkboxDeadlineResourceTrackerAccessPolicy | 2534 |
| 使用此策略 | 2534 |
| 策略详细信息 | 2534 |
| 策略版本 | 2534 |
| JSON 策略文档 | 2534 |
| 了解更多信息 | 2537 |

| | |
|--|------|
| AWSThinkboxDeadlineResourceTrackerAdminPolicy | 2537 |
| 使用此策略 | 2537 |
| 策略详细信息 | 2537 |
| 策略版本 | 2538 |
| JSON 策略文档 | 2538 |
| 了解更多信息 | 2543 |
| AWSThinkboxDeadlineSpotEventPluginAdminPolicy | 2544 |
| 使用此策略 | 2544 |
| 策略详细信息 | 2544 |
| 策略版本 | 2544 |
| JSON 策略文档 | 2544 |
| 了解更多信息 | 2547 |
| AWSThinkboxDeadlineSpotEventPluginWorkerPolicy | 2547 |
| 使用此策略 | 2547 |
| 策略详细信息 | 2547 |
| 策略版本 | 2548 |
| JSON 策略文档 | 2548 |
| 了解更多信息 | 2549 |
| AWSTransferConsoleFullAccess | 2549 |
| 使用此策略 | 2549 |
| 策略详细信息 | 2550 |
| 策略版本 | 2550 |
| JSON 策略文档 | 2550 |
| 了解更多信息 | 2551 |
| AWSTransferFullAccess | 2551 |
| 使用此策略 | 2551 |
| 策略详细信息 | 2551 |
| 策略版本 | 2551 |
| JSON 策略文档 | 2552 |
| 了解更多信息 | 2552 |
| AWSTransferLoggingAccess | 2553 |
| 使用此策略 | 2553 |
| 策略详细信息 | 2553 |
| 策略版本 | 2553 |
| JSON 策略文档 | 2553 |
| 了解更多信息 | 2554 |

| | |
|---|------|
| AWSTransferReadOnlyAccess | 2554 |
| 使用此策略 | 2554 |
| 策略详细信息 | 2554 |
| 策略版本 | 2554 |
| JSON 策略文档 | 2554 |
| 了解更多信息 | 2555 |
| AWSTrustedAdvisorPriorityFullAccess | 2555 |
| 使用此策略 | 2555 |
| 策略详细信息 | 2555 |
| 策略版本 | 2556 |
| JSON 策略文档 | 2556 |
| 了解更多信息 | 2557 |
| AWSTrustedAdvisorPriorityReadOnlyAccess | 2558 |
| 使用此策略 | 2558 |
| 策略详细信息 | 2558 |
| 策略版本 | 2558 |
| JSON 策略文档 | 2558 |
| 了解更多信息 | 2559 |
| AWSTrustedAdvisorReportingServiceRolePolicy | 2559 |
| 使用此策略 | 2560 |
| 策略详细信息 | 2560 |
| 策略版本 | 2560 |
| JSON 策略文档 | 2560 |
| 了解更多信息 | 2561 |
| AWSTrustedAdvisorServiceRolePolicy | 2561 |
| 使用此策略 | 2561 |
| 策略详细信息 | 2561 |
| 策略版本 | 2561 |
| JSON 策略文档 | 2561 |
| 了解更多信息 | 2564 |
| AWSUserNotificationsServiceLinkedRolePolicy | 2564 |
| 使用此策略 | 2564 |
| 策略详细信息 | 2564 |
| 策略版本 | 2565 |
| JSON 策略文档 | 2565 |
| 了解更多信息 | 2565 |

| | |
|---|------|
| AWSVendorInsightsAssessorFullAccess | 2566 |
| 使用此策略 | 2566 |
| 策略详细信息 | 2566 |
| 策略版本 | 2566 |
| JSON 策略文档 | 2566 |
| 了解更多信息 | 2567 |
| AWSVendorInsightsAssessorReadOnly | 2568 |
| 使用此策略 | 2568 |
| 策略详细信息 | 2568 |
| 策略版本 | 2568 |
| JSON 策略文档 | 2568 |
| 了解更多信息 | 2569 |
| AWSVendorInsightsVendorFullAccess | 2569 |
| 使用此策略 | 2569 |
| 策略详细信息 | 2569 |
| 策略版本 | 2569 |
| JSON 策略文档 | 2570 |
| 了解更多信息 | 2571 |
| AWSVendorInsightsVendorReadOnly | 2572 |
| 使用此策略 | 2572 |
| 策略详细信息 | 2572 |
| 策略版本 | 2572 |
| JSON 策略文档 | 2572 |
| 了解更多信息 | 2573 |
| AWSVpcLatticeServiceRolePolicy | 2573 |
| 使用此策略 | 2573 |
| 策略详细信息 | 2574 |
| 策略版本 | 2574 |
| JSON 策略文档 | 2574 |
| 了解更多信息 | 2574 |
| AWSVPCS2SVpnServiceRolePolicy | 2575 |
| 使用此策略 | 2575 |
| 策略详细信息 | 2575 |
| 策略版本 | 2575 |
| JSON 策略文档 | 2575 |
| 了解更多信息 | 2576 |

| | |
|---|------|
| AWSVPCTransitGatewayServiceRolePolicy | 2576 |
| 使用此策略 | 2576 |
| 策略详细信息 | 2576 |
| 策略版本 | 2576 |
| JSON 策略文档 | 2576 |
| 了解更多信息 | 2577 |
| AWSVPCVerifiedAccessServiceRolePolicy | 2577 |
| 使用此策略 | 2577 |
| 策略详细信息 | 2577 |
| 策略版本 | 2578 |
| JSON 策略文档 | 2578 |
| 了解更多信息 | 2579 |
| AWSWAFConsoleFullAccess | 2579 |
| 使用此策略 | 2580 |
| 策略详细信息 | 2580 |
| 策略版本 | 2580 |
| JSON 策略文档 | 2580 |
| 了解更多信息 | 2582 |
| AWSWAFConsoleReadOnlyAccess | 2582 |
| 使用此策略 | 2582 |
| 策略详细信息 | 2583 |
| 策略版本 | 2583 |
| JSON 策略文档 | 2583 |
| 了解更多信息 | 2584 |
| AWSWAFFullAccess | 2584 |
| 使用此策略 | 2584 |
| 策略详细信息 | 2584 |
| 策略版本 | 2584 |
| JSON 策略文档 | 2585 |
| 了解更多信息 | 2586 |
| AWSWAFReadOnlyAccess | 2586 |
| 使用此策略 | 2587 |
| 策略详细信息 | 2587 |
| 策略版本 | 2587 |
| JSON 策略文档 | 2587 |
| 了解更多信息 | 2588 |

| | |
|--|------|
| AWSWellArchitectedDiscoveryServiceRolePolicy | 2588 |
| 使用此策略 | 2588 |
| 策略详细信息 | 2588 |
| 策略版本 | 2588 |
| JSON 策略文档 | 2589 |
| 了解更多信息 | 2590 |
| AWSWellArchitectedOrganizationsServiceRolePolicy | 2590 |
| 使用此策略 | 2590 |
| 策略详细信息 | 2590 |
| 策略版本 | 2591 |
| JSON 策略文档 | 2591 |
| 了解更多信息 | 2591 |
| AWSWickrFullAccess | 2592 |
| 使用此策略 | 2592 |
| 策略详细信息 | 2592 |
| 策略版本 | 2592 |
| JSON 策略文档 | 2592 |
| 了解更多信息 | 2592 |
| AWSXrayCrossAccountSharingConfiguration | 2593 |
| 使用此策略 | 2593 |
| 策略详细信息 | 2593 |
| 策略版本 | 2593 |
| JSON 策略文档 | 2593 |
| 了解更多信息 | 2594 |
| AWSXRayDaemonWriteAccess | 2594 |
| 使用此策略 | 2594 |
| 策略详细信息 | 2595 |
| 策略版本 | 2595 |
| JSON 策略文档 | 2595 |
| 了解更多信息 | 2595 |
| AWSXrayFullAccess | 2596 |
| 使用此策略 | 2596 |
| 策略详细信息 | 2596 |
| 策略版本 | 2596 |
| JSON 策略文档 | 2596 |
| 了解更多信息 | 2597 |

| | |
|---|------|
| AWSXrayReadOnlyAccess | 2597 |
| 使用此策略 | 2597 |
| 策略详细信息 | 2597 |
| 策略版本 | 2597 |
| JSON 策略文档 | 2597 |
| 了解更多信息 | 2598 |
| AWSXrayWriteOnlyAccess | 2599 |
| 使用此策略 | 2599 |
| 策略详细信息 | 2599 |
| 策略版本 | 2599 |
| JSON 策略文档 | 2599 |
| 了解更多信息 | 2600 |
| AWSZonalAutoshiftPracticeRunSLRPolicy | 2600 |
| 使用此策略 | 2600 |
| 策略详细信息 | 2600 |
| 策略版本 | 2600 |
| JSON 策略文档 | 2600 |
| 了解更多信息 | 2601 |
| BatchServiceRolePolicy | 2601 |
| 使用此策略 | 2601 |
| 策略详细信息 | 2602 |
| 策略版本 | 2602 |
| JSON 策略文档 | 2602 |
| 了解更多信息 | 2608 |
| Billing | 2608 |
| 使用此策略 | 2608 |
| 策略详细信息 | 2608 |
| 策略版本 | 2609 |
| JSON 策略文档 | 2609 |
| 了解更多信息 | 2611 |
| CertificateManagerServiceRolePolicy | 2612 |
| 使用此策略 | 2612 |
| 策略详细信息 | 2612 |
| 策略版本 | 2612 |
| JSON 策略文档 | 2612 |
| 了解更多信息 | 2613 |

| | |
|---|------|
| ClientVPNServiceConnectionsRolePolicy | 2613 |
| 使用此策略 | 2613 |
| 策略详细信息 | 2613 |
| 策略版本 | 2613 |
| JSON 策略文档 | 2613 |
| 了解更多信息 | 2614 |
| ClientVPNServiceRolePolicy | 2614 |
| 使用此策略 | 2614 |
| 策略详细信息 | 2614 |
| 策略版本 | 2614 |
| JSON 策略文档 | 2614 |
| 了解更多信息 | 2615 |
| CloudFormationStackSetsOrgAdminServiceRolePolicy | 2615 |
| 使用此策略 | 2616 |
| 策略详细信息 | 2616 |
| 策略版本 | 2616 |
| JSON 策略文档 | 2616 |
| 了解更多信息 | 2617 |
| CloudFormationStackSetsOrgMemberServiceRolePolicy | 2617 |
| 使用此策略 | 2617 |
| 策略详细信息 | 2617 |
| 策略版本 | 2617 |
| JSON 策略文档 | 2617 |
| 了解更多信息 | 2618 |
| CloudFrontFullAccess | 2618 |
| 使用此策略 | 2618 |
| 策略详细信息 | 2619 |
| 策略版本 | 2619 |
| JSON 策略文档 | 2619 |
| 了解更多信息 | 2620 |
| CloudFrontReadOnlyAccess | 2620 |
| 使用此策略 | 2620 |
| 策略详细信息 | 2620 |
| 策略版本 | 2621 |
| JSON 策略文档 | 2621 |
| 了解更多信息 | 2622 |

| | |
|-------------------------------------|------|
| CloudHSMServiceRolePolicy | 2622 |
| 使用此策略 | 2622 |
| 策略详细信息 | 2622 |
| 策略版本 | 2622 |
| JSON 策略文档 | 2622 |
| 了解更多信息 | 2623 |
| CloudSearchFullAccess | 2623 |
| 使用此策略 | 2623 |
| 策略详细信息 | 2623 |
| 策略版本 | 2623 |
| JSON 策略文档 | 2624 |
| 了解更多信息 | 2624 |
| CloudSearchReadOnlyAccess | 2624 |
| 使用此策略 | 2624 |
| 策略详细信息 | 2624 |
| 策略版本 | 2625 |
| JSON 策略文档 | 2625 |
| 了解更多信息 | 2625 |
| CloudTrailServiceRolePolicy | 2625 |
| 使用此策略 | 2626 |
| 策略详细信息 | 2626 |
| 策略版本 | 2626 |
| JSON 策略文档 | 2626 |
| 了解更多信息 | 2628 |
| CloudWatch-CrossAccountAccess | 2628 |
| 使用此策略 | 2628 |
| 策略详细信息 | 2628 |
| 策略版本 | 2628 |
| JSON 策略文档 | 2628 |
| 了解更多信息 | 2629 |
| CloudWatchActionsEC2Access | 2629 |
| 使用此策略 | 2629 |
| 策略详细信息 | 2629 |
| 策略版本 | 2629 |
| JSON 策略文档 | 2630 |
| 了解更多信息 | 2630 |

| | |
|--|------|
| CloudWatchAgentAdminPolicy | 2630 |
| 使用此策略 | 2630 |
| 策略详细信息 | 2630 |
| 策略版本 | 2631 |
| JSON 策略文档 | 2631 |
| 了解更多信息 | 2632 |
| CloudWatchAgentServerPolicy | 2632 |
| 使用此策略 | 2632 |
| 策略详细信息 | 2632 |
| 策略版本 | 2632 |
| JSON 策略文档 | 2633 |
| 了解更多信息 | 2633 |
| CloudWatchApplicationInsightsFullAccess | 2634 |
| 使用此策略 | 2634 |
| 策略详细信息 | 2634 |
| 策略版本 | 2634 |
| JSON 策略文档 | 2634 |
| 了解更多信息 | 2636 |
| CloudWatchApplicationInsightsReadOnlyAccess | 2636 |
| 使用此策略 | 2636 |
| 策略详细信息 | 2636 |
| 策略版本 | 2636 |
| JSON 策略文档 | 2636 |
| 了解更多信息 | 2637 |
| CloudwatchApplicationInsightsServiceLinkedRolePolicy | 2637 |
| 使用此策略 | 2637 |
| 策略详细信息 | 2637 |
| 策略版本 | 2637 |
| JSON 策略文档 | 2638 |
| 了解更多信息 | 2647 |
| CloudWatchApplicationSignalsServiceRolePolicy | 2647 |
| 使用此策略 | 2648 |
| 策略详细信息 | 2648 |
| 策略版本 | 2648 |
| JSON 策略文档 | 2648 |
| 了解更多信息 | 2650 |

| | |
|--|------|
| CloudWatchAutomaticDashboardsAccess | 2650 |
| 使用此策略 | 2650 |
| 策略详细信息 | 2650 |
| 策略版本 | 2650 |
| JSON 策略文档 | 2650 |
| 了解更多信息 | 2652 |
| CloudWatchCrossAccountSharingConfiguration | 2652 |
| 使用此策略 | 2652 |
| 策略详细信息 | 2652 |
| 策略版本 | 2652 |
| JSON 策略文档 | 2653 |
| 了解更多信息 | 2653 |
| CloudWatchEventsBuiltInTargetExecutionAccess | 2654 |
| 使用此策略 | 2654 |
| 策略详细信息 | 2654 |
| 策略版本 | 2654 |
| JSON 策略文档 | 2654 |
| 了解更多信息 | 2655 |
| CloudWatchEventsFullAccess | 2655 |
| 使用此策略 | 2655 |
| 策略详细信息 | 2655 |
| 策略版本 | 2655 |
| JSON 策略文档 | 2656 |
| 了解更多信息 | 2657 |
| CloudWatchEventsInvocationAccess | 2658 |
| 使用此策略 | 2658 |
| 策略详细信息 | 2658 |
| 策略版本 | 2658 |
| JSON 策略文档 | 2658 |
| 了解更多信息 | 2659 |
| CloudWatchEventsReadOnlyAccess | 2659 |
| 使用此策略 | 2659 |
| 策略详细信息 | 2659 |
| 策略版本 | 2659 |
| JSON 策略文档 | 2660 |
| 了解更多信息 | 2661 |

| | |
|--|------|
| CloudWatchEventsServiceRolePolicy | 2661 |
| 使用此策略 | 2661 |
| 策略详细信息 | 2661 |
| 策略版本 | 2662 |
| JSON 策略文档 | 2662 |
| 了解更多信息 | 2662 |
| CloudWatchFullAccess | 2662 |
| 使用此策略 | 2663 |
| 策略详细信息 | 2663 |
| 策略版本 | 2663 |
| JSON 策略文档 | 2663 |
| 了解更多信息 | 2664 |
| CloudWatchFullAccessV2 | 2664 |
| 使用此策略 | 2664 |
| 策略详细信息 | 2664 |
| 策略版本 | 2665 |
| JSON 策略文档 | 2665 |
| 了解更多信息 | 2666 |
| CloudWatchInternetMonitorServiceRolePolicy | 2666 |
| 使用此策略 | 2667 |
| 策略详细信息 | 2667 |
| 策略版本 | 2667 |
| JSON 策略文档 | 2667 |
| 了解更多信息 | 2668 |
| CloudWatchLambdaInsightsExecutionRolePolicy | 2668 |
| 使用此策略 | 2668 |
| 策略详细信息 | 2668 |
| 策略版本 | 2669 |
| JSON 策略文档 | 2669 |
| 了解更多信息 | 2669 |
| CloudWatchLogsCrossAccountSharingConfiguration | 2670 |
| 使用此策略 | 2670 |
| 策略详细信息 | 2670 |
| 策略版本 | 2670 |
| JSON 策略文档 | 2670 |
| 了解更多信息 | 2671 |

| | |
|---|------|
| CloudWatchLogsFullAccess | 2671 |
| 使用此策略 | 2671 |
| 策略详细信息 | 2671 |
| 策略版本 | 2672 |
| JSON 策略文档 | 2672 |
| 了解更多信息 | 2672 |
| CloudWatchLogsReadOnlyAccess | 2672 |
| 使用此策略 | 2673 |
| 策略详细信息 | 2673 |
| 策略版本 | 2673 |
| JSON 策略文档 | 2673 |
| 了解更多信息 | 2674 |
| CloudWatchNetworkMonitorServiceRolePolicy | 2674 |
| 使用此策略 | 2674 |
| 策略详细信息 | 2674 |
| 策略版本 | 2674 |
| JSON 策略文档 | 2675 |
| 了解更多信息 | 2676 |
| CloudWatchReadOnlyAccess | 2676 |
| 使用此策略 | 2676 |
| 策略详细信息 | 2676 |
| 策略版本 | 2676 |
| JSON 策略文档 | 2677 |
| 了解更多信息 | 2678 |
| CloudWatchSyntheticsFullAccess | 2678 |
| 使用此策略 | 2678 |
| 策略详细信息 | 2678 |
| 策略版本 | 2678 |
| JSON 策略文档 | 2679 |
| 了解更多信息 | 2683 |
| CloudWatchSyntheticsReadOnlyAccess | 2683 |
| 使用此策略 | 2683 |
| 策略详细信息 | 2684 |
| 策略版本 | 2684 |
| JSON 策略文档 | 2684 |
| 了解更多信息 | 2684 |

| | |
|---|------|
| ComprehendDataAccessRolePolicy | 2685 |
| 使用此策略 | 2685 |
| 策略详细信息 | 2685 |
| 策略版本 | 2685 |
| JSON 策略文档 | 2685 |
| 了解更多信息 | 2686 |
| ComprehendFullAccess | 2686 |
| 使用此策略 | 2686 |
| 策略详细信息 | 2686 |
| 策略版本 | 2686 |
| JSON 策略文档 | 2686 |
| 了解更多信息 | 2687 |
| ComprehendMedicalFullAccess | 2687 |
| 使用此策略 | 2687 |
| 策略详细信息 | 2687 |
| 策略版本 | 2688 |
| JSON 策略文档 | 2688 |
| 了解更多信息 | 2688 |
| ComprehendReadOnly | 2688 |
| 使用此策略 | 2688 |
| 策略详细信息 | 2689 |
| 策略版本 | 2689 |
| JSON 策略文档 | 2689 |
| 了解更多信息 | 2690 |
| ComputeOptimizerReadOnlyAccess | 2690 |
| 使用此策略 | 2691 |
| 策略详细信息 | 2691 |
| 策略版本 | 2691 |
| JSON 策略文档 | 2691 |
| 了解更多信息 | 2692 |
| ComputeOptimizerServiceRolePolicy | 2692 |
| 使用此策略 | 2692 |
| 策略详细信息 | 2692 |
| 策略版本 | 2693 |
| JSON 策略文档 | 2693 |
| 了解更多信息 | 2694 |

| | |
|---|------|
| ConfigConformsServiceRolePolicy | 2694 |
| 使用此策略 | 2694 |
| 策略详细信息 | 2694 |
| 策略版本 | 2695 |
| JSON 策略文档 | 2695 |
| 了解更多信息 | 2698 |
| CostOptimizationHubAdminAccess | 2698 |
| 使用此策略 | 2698 |
| 策略详细信息 | 2698 |
| 策略版本 | 2698 |
| JSON 策略文档 | 2698 |
| 了解更多信息 | 2700 |
| CostOptimizationHubReadOnlyAccess | 2700 |
| 使用此策略 | 2700 |
| 策略详细信息 | 2700 |
| 策略版本 | 2700 |
| JSON 策略文档 | 2700 |
| 了解更多信息 | 2701 |
| CostOptimizationHubServiceRolePolicy | 2701 |
| 使用此策略 | 2701 |
| 策略详细信息 | 2701 |
| 策略版本 | 2702 |
| JSON 策略文档 | 2702 |
| 了解更多信息 | 2703 |
| CustomerProfilesServiceLinkedRolePolicy | 2703 |
| 使用此策略 | 2703 |
| 策略详细信息 | 2703 |
| 策略版本 | 2703 |
| JSON 策略文档 | 2703 |
| 了解更多信息 | 2704 |
| DatabaseAdministrator | 2704 |
| 使用此策略 | 2704 |
| 策略详细信息 | 2704 |
| 策略版本 | 2705 |
| JSON 策略文档 | 2705 |
| 了解更多信息 | 2707 |

| | |
|--|------|
| DataScientist | 2707 |
| 使用此策略 | 2707 |
| 策略详细信息 | 2707 |
| 策略版本 | 2708 |
| JSON 策略文档 | 2708 |
| 了解更多信息 | 2712 |
| DAXServiceRolePolicy | 2712 |
| 使用此策略 | 2712 |
| 策略详细信息 | 2712 |
| 策略版本 | 2712 |
| JSON 策略文档 | 2712 |
| 了解更多信息 | 2713 |
| DynamoDBCloudWatchContributorInsightsServiceRolePolicy | 2713 |
| 使用此策略 | 2713 |
| 策略详细信息 | 2713 |
| 策略版本 | 2714 |
| JSON 策略文档 | 2714 |
| 了解更多信息 | 2714 |
| DynamoDBKinesisReplicationServiceRolePolicy | 2715 |
| 使用此策略 | 2715 |
| 策略详细信息 | 2715 |
| 策略版本 | 2715 |
| JSON 策略文档 | 2715 |
| 了解更多信息 | 2716 |
| DynamoDBReplicationServiceRolePolicy | 2716 |
| 使用此策略 | 2716 |
| 策略详细信息 | 2716 |
| 策略版本 | 2716 |
| JSON 策略文档 | 2717 |
| 了解更多信息 | 2718 |
| EC2FastLaunchServiceRolePolicy | 2718 |
| 使用此策略 | 2718 |
| 策略详细信息 | 2718 |
| 策略版本 | 2718 |
| JSON 策略文档 | 2719 |
| 了解更多信息 | 2722 |

| | |
|---|------|
| EC2FleetTimeShiftableServiceRolePolicy | 2723 |
| 使用此策略 | 2723 |
| 策略详细信息 | 2723 |
| 策略版本 | 2723 |
| JSON 策略文档 | 2723 |
| 了解更多信息 | 2725 |
| Ec2ImageBuilderCrossAccountDistributionAccess | 2725 |
| 使用此策略 | 2725 |
| 策略详细信息 | 2725 |
| 策略版本 | 2725 |
| JSON 策略文档 | 2725 |
| 了解更多信息 | 2726 |
| EC2ImageBuilderLifecycleExecutionPolicy | 2726 |
| 使用此策略 | 2726 |
| 策略详细信息 | 2726 |
| 策略版本 | 2727 |
| JSON 策略文档 | 2727 |
| 了解更多信息 | 2729 |
| EC2InstanceConnect | 2729 |
| 使用此策略 | 2729 |
| 策略详细信息 | 2729 |
| 策略版本 | 2729 |
| JSON 策略文档 | 2729 |
| 了解更多信息 | 2730 |
| Ec2InstanceConnectEndpoint | 2730 |
| 使用此策略 | 2730 |
| 策略详细信息 | 2730 |
| 策略版本 | 2730 |
| JSON 策略文档 | 2731 |
| 了解更多信息 | 2733 |
| EC2InstanceProfileForImageBuilder | 2733 |
| 使用此策略 | 2733 |
| 策略详细信息 | 2733 |
| 策略版本 | 2733 |
| JSON 策略文档 | 2733 |
| 了解更多信息 | 2734 |

| | |
|---|------|
| EC2InstanceProfileForImageBuilderECRContainerBuilds | 2735 |
| 使用此策略 | 2735 |
| 策略详细信息 | 2735 |
| 策略版本 | 2735 |
| JSON 策略文档 | 2735 |
| 了解更多信息 | 2737 |
| ECRReplicationServiceRolePolicy | 2737 |
| 使用此策略 | 2737 |
| 策略详细信息 | 2737 |
| 策略版本 | 2737 |
| JSON 策略文档 | 2737 |
| 了解更多信息 | 2738 |
| ElastiCacheServiceRolePolicy | 2738 |
| 使用此策略 | 2738 |
| 策略详细信息 | 2738 |
| 策略版本 | 2738 |
| JSON 策略文档 | 2739 |
| 了解更多信息 | 2741 |
| ElasticLoadBalancingFullAccess | 2741 |
| 使用此策略 | 2741 |
| 策略详细信息 | 2741 |
| 策略版本 | 2741 |
| JSON 策略文档 | 2741 |
| 了解更多信息 | 2743 |
| ElasticLoadBalancingReadOnly | 2743 |
| 使用此策略 | 2743 |
| 策略详细信息 | 2743 |
| 策略版本 | 2743 |
| JSON 策略文档 | 2743 |
| 了解更多信息 | 2744 |
| ElementalActivationsDownloadSoftwareAccess | 2745 |
| 使用此策略 | 2745 |
| 策略详细信息 | 2745 |
| 策略版本 | 2745 |
| JSON 策略文档 | 2745 |
| 了解更多信息 | 2746 |

| | |
|---|------|
| ElementalActivationsFullAccess | 2746 |
| 使用此策略 | 2746 |
| 策略详细信息 | 2746 |
| 策略版本 | 2746 |
| JSON 策略文档 | 2746 |
| 了解更多信息 | 2747 |
| ElementalActivationsGenerateLicenses | 2747 |
| 使用此策略 | 2747 |
| 策略详细信息 | 2747 |
| 策略版本 | 2747 |
| JSON 策略文档 | 2748 |
| 了解更多信息 | 2748 |
| ElementalActivationsReadOnlyAccess | 2748 |
| 使用此策略 | 2748 |
| 策略详细信息 | 2749 |
| 策略版本 | 2749 |
| JSON 策略文档 | 2749 |
| 了解更多信息 | 2749 |
| ElementalAppliancesSoftwareFullAccess | 2750 |
| 使用此策略 | 2750 |
| 策略详细信息 | 2750 |
| 策略版本 | 2750 |
| JSON 策略文档 | 2750 |
| 了解更多信息 | 2751 |
| ElementalAppliancesSoftwareReadOnlyAccess | 2751 |
| 使用此策略 | 2751 |
| 策略详细信息 | 2751 |
| 策略版本 | 2751 |
| JSON 策略文档 | 2751 |
| 了解更多信息 | 2752 |
| ElementalSupportCenterFullAccess | 2752 |
| 使用此策略 | 2752 |
| 策略详细信息 | 2752 |
| 策略版本 | 2752 |
| JSON 策略文档 | 2753 |
| 了解更多信息 | 2753 |

| | |
|---|------|
| EMRDescribeClusterPolicyForEMRWAL | 2753 |
| 使用此策略 | 2753 |
| 策略详细信息 | 2753 |
| 策略版本 | 2754 |
| JSON 策略文档 | 2754 |
| 了解更多信息 | 2754 |
| FMSServiceRolePolicy | 2754 |
| 使用此策略 | 2754 |
| 策略详细信息 | 2755 |
| 策略版本 | 2755 |
| JSON 策略文档 | 2755 |
| 了解更多信息 | 2769 |
| FSxDeleteServiceLinkedRoleAccess | 2769 |
| 使用此策略 | 2769 |
| 策略详细信息 | 2769 |
| 策略版本 | 2770 |
| JSON 策略文档 | 2770 |
| 了解更多信息 | 2770 |
| GameLiftGameServerGroupPolicy | 2770 |
| 使用此策略 | 2770 |
| 策略详细信息 | 2771 |
| 策略版本 | 2771 |
| JSON 策略文档 | 2771 |
| 了解更多信息 | 2772 |
| GlobalAcceleratorFullAccess | 2773 |
| 使用此策略 | 2773 |
| 策略详细信息 | 2773 |
| 策略版本 | 2773 |
| JSON 策略文档 | 2773 |
| 了解更多信息 | 2774 |
| GlobalAcceleratorReadOnlyAccess | 2775 |
| 使用此策略 | 2775 |
| 策略详细信息 | 2775 |
| 策略版本 | 2775 |
| JSON 策略文档 | 2775 |
| 了解更多信息 | 2776 |

| | |
|---|------|
| GreengrassOTAUpdateArtifactAccess | 2776 |
| 使用此策略 | 2776 |
| 策略详细信息 | 2776 |
| 策略版本 | 2776 |
| JSON 策略文档 | 2776 |
| 了解更多信息 | 2777 |
| GroundTruthSyntheticConsoleFullAccess | 2777 |
| 使用此策略 | 2777 |
| 策略详细信息 | 2777 |
| 策略版本 | 2777 |
| JSON 策略文档 | 2778 |
| 了解更多信息 | 2778 |
| GroundTruthSyntheticConsoleReadOnlyAccess | 2778 |
| 使用此策略 | 2778 |
| 策略详细信息 | 2778 |
| 策略版本 | 2779 |
| JSON 策略文档 | 2779 |
| 了解更多信息 | 2779 |
| Health_OrganizationsServiceRolePolicy | 2779 |
| 使用此策略 | 2780 |
| 策略详细信息 | 2780 |
| 策略版本 | 2780 |
| JSON 策略文档 | 2780 |
| 了解更多信息 | 2781 |
| IAMAccessAdvisorReadOnly | 2781 |
| 使用此策略 | 2781 |
| 策略详细信息 | 2781 |
| 策略版本 | 2781 |
| JSON 策略文档 | 2781 |
| 了解更多信息 | 2782 |
| IAMAccessAnalyzerFullAccess | 2782 |
| 使用此策略 | 2783 |
| 策略详细信息 | 2783 |
| 策略版本 | 2783 |
| JSON 策略文档 | 2783 |
| 了解更多信息 | 2784 |

| | |
|---|------|
| IAMAccessAnalyzerReadOnlyAccess | 2784 |
| 使用此策略 | 2784 |
| 策略详细信息 | 2784 |
| 策略版本 | 2785 |
| JSON 策略文档 | 2785 |
| 了解更多信息 | 2785 |
| IAMFullAccess | 2786 |
| 使用此策略 | 2786 |
| 策略详细信息 | 2786 |
| 策略版本 | 2786 |
| JSON 策略文档 | 2786 |
| 了解更多信息 | 2787 |
| IAMReadOnlyAccess | 2787 |
| 使用此策略 | 2787 |
| 策略详细信息 | 2787 |
| 策略版本 | 2787 |
| JSON 策略文档 | 2788 |
| 了解更多信息 | 2788 |
| IAMSelfManageServiceSpecificCredentials | 2788 |
| 使用此策略 | 2788 |
| 策略详细信息 | 2789 |
| 策略版本 | 2789 |
| JSON 策略文档 | 2789 |
| 了解更多信息 | 2789 |
| IAMUserChangePassword | 2790 |
| 使用此策略 | 2790 |
| 策略详细信息 | 2790 |
| 策略版本 | 2790 |
| JSON 策略文档 | 2790 |
| 了解更多信息 | 2791 |
| IAMUserSSHKeys | 2791 |
| 使用此策略 | 2791 |
| 策略详细信息 | 2791 |
| 策略版本 | 2791 |
| JSON 策略文档 | 2792 |
| 了解更多信息 | 2792 |

| | |
|---|------|
| IVSFullAccess | 2792 |
| 使用此策略 | 2792 |
| 策略详细信息 | 2792 |
| 策略版本 | 2793 |
| JSON 策略文档 | 2793 |
| 了解更多信息 | 2793 |
| IVSReadOnlyAccess | 2793 |
| 使用此策略 | 2794 |
| 策略详细信息 | 2794 |
| 策略版本 | 2794 |
| JSON 策略文档 | 2794 |
| 了解更多信息 | 2795 |
| IVSRecordToS3 | 2795 |
| 使用此策略 | 2795 |
| 策略详细信息 | 2795 |
| 策略版本 | 2796 |
| JSON 策略文档 | 2796 |
| 了解更多信息 | 2796 |
| KafkaConnectServiceRolePolicy | 2796 |
| 使用此策略 | 2797 |
| 策略详细信息 | 2797 |
| 策略版本 | 2797 |
| JSON 策略文档 | 2797 |
| 了解更多信息 | 2798 |
| KafkaServiceRolePolicy | 2799 |
| 使用此策略 | 2799 |
| 策略详细信息 | 2799 |
| 策略版本 | 2799 |
| JSON 策略文档 | 2799 |
| 了解更多信息 | 2801 |
| KeyspacesReplicationServiceRolePolicy | 2801 |
| 使用此策略 | 2801 |
| 策略详细信息 | 2801 |
| 策略版本 | 2801 |
| JSON 策略文档 | 2801 |
| 了解更多信息 | 2802 |

| | |
|--|------|
| LakeFormationDataAccessServiceRolePolicy | 2802 |
| 使用此策略 | 2802 |
| 策略详细信息 | 2802 |
| 策略版本 | 2802 |
| JSON 策略文档 | 2803 |
| 了解更多信息 | 2803 |
| LexBotPolicy | 2803 |
| 使用此策略 | 2803 |
| 策略详细信息 | 2803 |
| 策略版本 | 2804 |
| JSON 策略文档 | 2804 |
| 了解更多信息 | 2804 |
| LexChannelPolicy | 2805 |
| 使用此策略 | 2805 |
| 策略详细信息 | 2805 |
| 策略版本 | 2805 |
| JSON 策略文档 | 2805 |
| 了解更多信息 | 2806 |
| LightsailExportAccess | 2806 |
| 使用此策略 | 2806 |
| 策略详细信息 | 2806 |
| 策略版本 | 2806 |
| JSON 策略文档 | 2806 |
| 了解更多信息 | 2807 |
| MediaConnectGatewayInstanceRolePolicy | 2807 |
| 使用此策略 | 2807 |
| 策略详细信息 | 2807 |
| 策略版本 | 2808 |
| JSON 策略文档 | 2808 |
| 了解更多信息 | 2808 |
| MediaPackageServiceRolePolicy | 2809 |
| 使用此策略 | 2809 |
| 策略详细信息 | 2809 |
| 策略版本 | 2809 |
| JSON 策略文档 | 2809 |
| 了解更多信息 | 2810 |

| | |
|--|------|
| MemoryDBServiceRolePolicy | 2810 |
| 使用此策略 | 2810 |
| 策略详细信息 | 2810 |
| 策略版本 | 2810 |
| JSON 策略文档 | 2810 |
| 了解更多信息 | 2812 |
| MigrationHubDMSAccessServiceRolePolicy | 2813 |
| 使用此策略 | 2813 |
| 策略详细信息 | 2813 |
| 策略版本 | 2813 |
| JSON 策略文档 | 2813 |
| 了解更多信息 | 2814 |
| MigrationHubServiceRolePolicy | 2814 |
| 使用此策略 | 2814 |
| 策略详细信息 | 2814 |
| 策略版本 | 2815 |
| JSON 策略文档 | 2815 |
| 了解更多信息 | 2816 |
| MigrationHubSMSAccessServiceRolePolicy | 2816 |
| 使用此策略 | 2816 |
| 策略详细信息 | 2816 |
| 策略版本 | 2817 |
| JSON 策略文档 | 2817 |
| 了解更多信息 | 2818 |
| MonitronServiceRolePolicy | 2818 |
| 使用此策略 | 2818 |
| 策略详细信息 | 2818 |
| 策略版本 | 2818 |
| JSON 策略文档 | 2819 |
| 了解更多信息 | 2819 |
| NeptuneConsoleFullAccess | 2819 |
| 使用此策略 | 2819 |
| 策略详细信息 | 2819 |
| 策略版本 | 2820 |
| JSON 策略文档 | 2820 |
| 了解更多信息 | 2825 |

| | |
|----------------------------------|------|
| NeptuneFullAccess | 2826 |
| 使用此策略 | 2826 |
| 策略详细信息 | 2826 |
| 策略版本 | 2826 |
| JSON 策略文档 | 2826 |
| 了解更多信息 | 2830 |
| NeptuneGraphReadOnlyAccess | 2830 |
| 使用此策略 | 2830 |
| 策略详细信息 | 2830 |
| 策略版本 | 2831 |
| JSON 策略文档 | 2831 |
| 了解更多信息 | 2832 |
| NeptuneReadOnlyAccess | 2833 |
| 使用此策略 | 2833 |
| 策略详细信息 | 2833 |
| 策略版本 | 2833 |
| JSON 策略文档 | 2833 |
| 了解更多信息 | 2835 |
| NetworkAdministrator | 2836 |
| 使用此策略 | 2836 |
| 策略详细信息 | 2836 |
| 策略版本 | 2836 |
| JSON 策略文档 | 2836 |
| 了解更多信息 | 2843 |
| OAMFullAccess | 2843 |
| 使用此策略 | 2843 |
| 策略详细信息 | 2843 |
| 策略版本 | 2843 |
| JSON 策略文档 | 2843 |
| 了解更多信息 | 2844 |
| OAMReadOnlyAccess | 2844 |
| 使用此策略 | 2844 |
| 策略详细信息 | 2844 |
| 策略版本 | 2844 |
| JSON 策略文档 | 2845 |
| 了解更多信息 | 2845 |

| | |
|---|------|
| PartnerCentralAccountManagementUserRoleAssociation | 2845 |
| 使用此策略 | 2845 |
| 策略详细信息 | 2845 |
| 策略版本 | 2846 |
| JSON 策略文档 | 2846 |
| 了解更多信息 | 2847 |
| PowerUserAccess | 2847 |
| 使用此策略 | 2847 |
| 策略详细信息 | 2847 |
| 策略版本 | 2847 |
| JSON 策略文档 | 2847 |
| 了解更多信息 | 2848 |
| QuickSightAccessForS3StorageManagementAnalyticsReadOnly | 2848 |
| 使用此策略 | 2848 |
| 策略详细信息 | 2849 |
| 策略版本 | 2849 |
| JSON 策略文档 | 2849 |
| 了解更多信息 | 2850 |
| RDSCloudHsmAuthorizationRole | 2850 |
| 使用此策略 | 2850 |
| 策略详细信息 | 2850 |
| 策略版本 | 2850 |
| JSON 策略文档 | 2850 |
| 了解更多信息 | 2851 |
| ReadOnlyAccess | 2851 |
| 使用此策略 | 2851 |
| 策略详细信息 | 2851 |
| 策略版本 | 2851 |
| JSON 策略文档 | 2852 |
| 了解更多信息 | 2898 |
| ResourceGroupsandTagEditorFullAccess | 2898 |
| 使用此策略 | 2898 |
| 策略详细信息 | 2898 |
| 策略版本 | 2899 |
| JSON 策略文档 | 2899 |
| 了解更多信息 | 2899 |

| | |
|--|------|
| ResourceGroupsandTagEditorReadOnlyAccess | 2900 |
| 使用此策略 | 2900 |
| 策略详细信息 | 2900 |
| 策略版本 | 2900 |
| JSON 策略文档 | 2900 |
| 了解更多信息 | 2901 |
| ResourceGroupsServiceRolePolicy | 2901 |
| 使用此策略 | 2901 |
| 策略详细信息 | 2901 |
| 策略版本 | 2901 |
| JSON 策略文档 | 2902 |
| 了解更多信息 | 2902 |
| ROSAAmazonEBSCSIDriverOperatorPolicy | 2902 |
| 使用此策略 | 2902 |
| 策略详细信息 | 2902 |
| 策略版本 | 2903 |
| JSON 策略文档 | 2903 |
| 了解更多信息 | 2906 |
| ROSACloudNetworkConfigOperatorPolicy | 2906 |
| 使用此策略 | 2906 |
| 策略详细信息 | 2906 |
| 策略版本 | 2906 |
| JSON 策略文档 | 2907 |
| 了解更多信息 | 2907 |
| ROSAControlPlaneOperatorPolicy | 2908 |
| 使用此策略 | 2908 |
| 策略详细信息 | 2908 |
| 策略版本 | 2908 |
| JSON 策略文档 | 2908 |
| 了解更多信息 | 2913 |
| ROSAImageRegistryOperatorPolicy | 2913 |
| 使用此策略 | 2913 |
| 策略详细信息 | 2913 |
| 策略版本 | 2913 |
| JSON 策略文档 | 2914 |
| 了解更多信息 | 2915 |

| | |
|------------------------------------|------|
| ROSAIngressOperatorPolicy | 2915 |
| 使用此策略 | 2915 |
| 策略详细信息 | 2915 |
| 策略版本 | 2915 |
| JSON 策略文档 | 2916 |
| 了解更多信息 | 2916 |
| ROSAInstallerPolicy | 2917 |
| 使用此策略 | 2917 |
| 策略详细信息 | 2917 |
| 策略版本 | 2917 |
| JSON 策略文档 | 2917 |
| 了解更多信息 | 2924 |
| ROSAKMSProviderPolicy | 2925 |
| 使用此策略 | 2925 |
| 策略详细信息 | 2925 |
| 策略版本 | 2925 |
| JSON 策略文档 | 2925 |
| 了解更多信息 | 2926 |
| ROSAKubeControllerPolicy | 2926 |
| 使用此策略 | 2926 |
| 策略详细信息 | 2926 |
| 策略版本 | 2926 |
| JSON 策略文档 | 2927 |
| 了解更多信息 | 2931 |
| ROSAManageSubscription | 2931 |
| 使用此策略 | 2931 |
| 策略详细信息 | 2931 |
| 策略版本 | 2932 |
| JSON 策略文档 | 2932 |
| 了解更多信息 | 2932 |
| ROSANodePoolManagementPolicy | 2933 |
| 使用此策略 | 2933 |
| 策略详细信息 | 2933 |
| 策略版本 | 2933 |
| JSON 策略文档 | 2933 |
| 了解更多信息 | 2939 |

| | |
|---|------|
| ROSASRESupportPolicy | 2939 |
| 使用此策略 | 2939 |
| 策略详细信息 | 2939 |
| 策略版本 | 2940 |
| JSON 策略文档 | 2940 |
| 了解更多信息 | 2944 |
| ROSAWorkerInstancePolicy | 2945 |
| 使用此策略 | 2945 |
| 策略详细信息 | 2945 |
| 策略版本 | 2945 |
| JSON 策略文档 | 2945 |
| 了解更多信息 | 2946 |
| Route53RecoveryReadinessServiceRolePolicy | 2946 |
| 使用此策略 | 2946 |
| 策略详细信息 | 2946 |
| 策略版本 | 2946 |
| JSON 策略文档 | 2947 |
| 了解更多信息 | 2950 |
| Route53ResolverServiceRolePolicy | 2950 |
| 使用此策略 | 2950 |
| 策略详细信息 | 2950 |
| 策略版本 | 2951 |
| JSON 策略文档 | 2951 |
| 了解更多信息 | 2951 |
| S3StorageLensServiceRolePolicy | 2952 |
| 使用此策略 | 2952 |
| 策略详细信息 | 2952 |
| 策略版本 | 2952 |
| JSON 策略文档 | 2952 |
| 了解更多信息 | 2953 |
| SecretsManagerReadWrite | 2953 |
| 使用此策略 | 2953 |
| 策略详细信息 | 2953 |
| 策略版本 | 2953 |
| JSON 策略文档 | 2953 |
| 了解更多信息 | 2955 |

| | |
|---|------|
| SecurityAudit | 2955 |
| 使用此策略 | 2955 |
| 策略详细信息 | 2955 |
| 策略版本 | 2956 |
| JSON 策略文档 | 2956 |
| 了解更多信息 | 2971 |
| SecurityLakeServiceLinkedRole | 2972 |
| 使用此策略 | 2972 |
| 策略详细信息 | 2972 |
| 策略版本 | 2972 |
| JSON 策略文档 | 2972 |
| 了解更多信息 | 2975 |
| ServerMigration_ServiceRole | 2975 |
| 使用此策略 | 2975 |
| 策略详细信息 | 2975 |
| 策略版本 | 2975 |
| JSON 策略文档 | 2975 |
| 了解更多信息 | 2980 |
| ServerMigrationConnector | 2980 |
| 使用此策略 | 2980 |
| 策略详细信息 | 2981 |
| 策略版本 | 2981 |
| JSON 策略文档 | 2981 |
| 了解更多信息 | 2982 |
| ServerMigrationServiceConsoleFullAccess | 2983 |
| 使用此策略 | 2983 |
| 策略详细信息 | 2983 |
| 策略版本 | 2983 |
| JSON 策略文档 | 2983 |
| 了解更多信息 | 2985 |
| ServerMigrationServiceLaunchRole | 2985 |
| 使用此策略 | 2985 |
| 策略详细信息 | 2985 |
| 策略版本 | 2985 |
| JSON 策略文档 | 2986 |
| 了解更多信息 | 2988 |

| | |
|---|------|
| ServerMigrationServiceRoleForInstanceValidation | 2988 |
| 使用此策略 | 2989 |
| 策略详细信息 | 2989 |
| 策略版本 | 2989 |
| JSON 策略文档 | 2989 |
| 了解更多信息 | 2990 |
| ServiceQuotasFullAccess | 2990 |
| 使用此策略 | 2990 |
| 策略详细信息 | 2990 |
| 策略版本 | 2990 |
| JSON 策略文档 | 2990 |
| 了解更多信息 | 2992 |
| ServiceQuotasReadOnlyAccess | 2992 |
| 使用此策略 | 2992 |
| 策略详细信息 | 2992 |
| 策略版本 | 2993 |
| JSON 策略文档 | 2993 |
| 了解更多信息 | 2994 |
| ServiceQuotasServiceRolePolicy | 2994 |
| 使用此策略 | 2994 |
| 策略详细信息 | 2994 |
| 策略版本 | 2994 |
| JSON 策略文档 | 2995 |
| 了解更多信息 | 2995 |
| SimpleWorkflowFullAccess | 2995 |
| 使用此策略 | 2995 |
| 策略详细信息 | 2995 |
| 策略版本 | 2996 |
| JSON 策略文档 | 2996 |
| 了解更多信息 | 2996 |
| SupportUser | 2996 |
| 使用此策略 | 2996 |
| 策略详细信息 | 2997 |
| 策略版本 | 2997 |
| JSON 策略文档 | 2997 |
| 了解更多信息 | 3002 |

| | |
|---|------|
| SystemAdministrator | 3002 |
| 使用此策略 | 3002 |
| 策略详细信息 | 3002 |
| 策略版本 | 3002 |
| JSON 策略文档 | 3003 |
| 了解更多信息 | 3009 |
| TranslateFullAccess | 3009 |
| 使用此策略 | 3009 |
| 策略详细信息 | 3009 |
| 策略版本 | 3009 |
| JSON 策略文档 | 3009 |
| 了解更多信息 | 3010 |
| TranslateReadOnly | 3010 |
| 使用此策略 | 3010 |
| 策略详细信息 | 3010 |
| 策略版本 | 3011 |
| JSON 策略文档 | 3011 |
| 了解更多信息 | 3011 |
| ViewOnlyAccess | 3012 |
| 使用此策略 | 3012 |
| 策略详细信息 | 3012 |
| 策略版本 | 3012 |
| JSON 策略文档 | 3012 |
| 了解更多信息 | 3018 |
| VMImportExportRoleForAWSConnector | 3018 |
| 使用此策略 | 3018 |
| 策略详细信息 | 3018 |
| 策略版本 | 3019 |
| JSON 策略文档 | 3019 |
| 了解更多信息 | 3020 |
| VPCLatticeFullAccess | 3020 |
| 使用此策略 | 3020 |
| 策略详细信息 | 3020 |
| 策略版本 | 3020 |
| JSON 策略文档 | 3020 |
| 了解更多信息 | 3022 |

| | |
|---|------|
| VPCLatticeReadOnlyAccess | 3023 |
| 使用此策略 | 3023 |
| 策略详细信息 | 3023 |
| 策略版本 | 3023 |
| JSON 策略文档 | 3023 |
| 了解更多信息 | 3024 |
| VPCLatticeServicesInvokeAccess | 3024 |
| 使用此策略 | 3024 |
| 策略详细信息 | 3024 |
| 策略版本 | 3025 |
| JSON 策略文档 | 3025 |
| 了解更多信息 | 3025 |
| WAFLoggingServiceRolePolicy | 3025 |
| 使用此策略 | 3025 |
| 策略详细信息 | 3026 |
| 策略版本 | 3026 |
| JSON 策略文档 | 3026 |
| 了解更多信息 | 3026 |
| WAFRegionalLoggingServiceRolePolicy | 3027 |
| 使用此策略 | 3027 |
| 策略详细信息 | 3027 |
| 策略版本 | 3027 |
| JSON 策略文档 | 3027 |
| 了解更多信息 | 3028 |
| WAFV2LoggingServiceRolePolicy | 3028 |
| 使用此策略 | 3028 |
| 策略详细信息 | 3028 |
| 策略版本 | 3028 |
| JSON 策略文档 | 3028 |
| 了解更多信息 | 3029 |
| WellArchitectedConsoleFullAccess | 3029 |
| 使用此策略 | 3029 |
| 策略详细信息 | 3029 |
| 策略版本 | 3030 |
| JSON 策略文档 | 3030 |
| 了解更多信息 | 3030 |

| | |
|--|----------|
| WellArchitectedConsoleReadOnlyAccess | 3030 |
| 使用此策略 | 3030 |
| 策略详细信息 | 3031 |
| 策略版本 | 3031 |
| JSON 策略文档 | 3031 |
| 了解更多信息 | 3031 |
| WorkLinkServiceRolePolicy | 3032 |
| 使用此策略 | 3032 |
| 策略详细信息 | 3032 |
| 策略版本 | 3032 |
| JSON 策略文档 | 3032 |
| 了解更多信息 | 3033 |
| | mmmxxxiv |

什么是 AWS 托管策略？

AWS 托管策略是由 AWS 创建和管理的独立策略。AWS 托管策略旨在为许多常见使用案例提供权限。与必须自己编写策略相比，通过托管策略可以更轻松地将权限分配给用户、组和角色。

请记住，AWS 托管策略可能不会为您的特定使用场景授予最低权限许可，因为它们可供所有 AWS 客户使用。建议通过定义特定于您的应用场景的[客户托管策略](#)来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新在 AWS 托管策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)。

了解策略参考页面

每个策略参考页面均包含以下信息：

- 使用此策略 – 是否可以将此策略附加到用户、组和角色
- 策略详细信息
 - 类型 - AWS 托管策略的类型
 - AWS managed policy – 标准 AWS 托管策略
 - Job function policy – 贴合行业中常用工作职能的策略
 - Service-linked role policy – 附加到服务相关角色的策略允许服务代表您执行操作，例如 [the section called “AmazonRDSPreviewServiceRolePolicy”](#)
 - Service role policy – 旨在与服务角色配合使用的策略，例如 [the section called “AWSControlTowerServiceRolePolicy”](#)
 - 创建时间 – 首次创建此策略的时间
 - 编辑时间 – 编辑此版本策略的时间
 - ARN – 策略的 Amazon 资源名称
- 策略版本 – 策略授予的权限版本
- JSON 策略文档 – 策略 JSON
- 了解更多 – 与 AWS 托管策略相关的文档链接

已弃用的 AWS 托管策略

AWS 定期更新 AWS 托管策略。大多数情况下，我们会向策略添加权限。当推出新的服务或功能时，我们会添加权限。为了提高 AWS 托管策略的安全性，我们有时会减小策略的范围。在删除策略权限后，我们将该策略设置为已弃用状态，并提供一个新的可用策略。在 AWS 弃用某项服务或功能后，我们也会弃用该功能的 AWS 托管策略。

如果您收到一封电子邮件通知，告知您正在使用的策略已弃用，我们建议您立即采取行动。确定策略的变更并更新您的工作流。如果 AWS 提供了替代策略，则计划将其附加到所有受影响的身份（用户、组和角色），然后将已弃用的策略与这些身份分离。

已弃用的策略具有以下特性：

- 已从本指南中删除。
- 对于所有当前已附加该策略的身份，权限仍然有效。
- 在已附加该策略的身份所在的账户中，该策略将显示在 IAM 控制台的策略列表中，旁边有一个警告图标。
- 它无法附加至任何新身份。该策略若与当前身份分离则不能重新附加。
- 在与所有当前实体分离以后，该策略将不再显示。

AWS 托管策略

AWS 托管策略

- [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](#)
- [AmazonEKSConectorServiceRolePolicy](#)
- [AmazonEKSFargatePodExecutionRolePolicy](#)
- [AmazonEKSTaskExecutionRolePolicy](#)
- [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](#)
- [AmazonSESEFullAccess](#)
- [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](#)
- [AWSApplicationAutoscalingElastiCacheRGPPolicy](#)
- [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](#)
- [AWSCertificateManagerPrivateCARedOnly](#)
- [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](#)
- [AWSIoTTOTAUpdate](#)
- [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](#)
- [AWSResilienceHubAssessmentExecutionPolicy](#)
- [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](#)
- [ROSAKMSPProviderPolicy](#)
- [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](#)
- [VPC_LatticeFullAccess](#)
- [VPC_LatticeReadOnlyAccess](#)
- [VPC_LatticeServicesInvokeAccess](#)
- [WAFLoggingServiceRolePolicy](#)
- [WAFRegionalLoggingServiceRolePolicy](#)
- [WAFV2LoggingServiceRolePolicy](#)
- [WellArchitectedConsoleFullAccess](#)
- [WellArchitectedConsoleReadOnlyAccess](#)
- [WorkLinkServiceRolePolicy](#)

AccessAnalyzerServiceRolePolicy

AccessAnalyzerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Access Analyzer 分析资源元数据

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 2 日 17:13 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 22:34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

策略版本

策略版本：v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AdministratorAccess

AdministratorAccess 是一种 [AWS 托管策略](#)，它：提供对 AWS 服务和资源的完全访问权限。

使用此策略

您可以将 AdministratorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AdministratorAccess-Amplify

AdministratorAccess-Amplify 是一项 [AWS 托管策略](#)：授予账户管理权限，同时明确允许直接访问 Amplify 应用程序所需的资源。

使用此策略

您可以将 AdministratorAccess-Amplify 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 19:03 UTC
- 编辑时间：2023 年 5 月 31 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-Amplify

策略版本

策略版本 : v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:AdminListGroupForUser",
  "cognito-idp:ListGroup",
  "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:*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AdministratorAccess-AWSElasticBeanstalk

AdministratorAccess-AWSElasticBeanstalk 是一项 [AWS 托管策略](#)：授予账户管理权限。明确允许开发人员和管理员直接访问管理 AWS Elastic Beanstalk 应用程序所需的资源

使用此策略

您可以将 AdministratorAccess-AWSElasticBeanstalk 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 19:36 UTC

- 编辑时间：2023 年 3 月 23 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessDeviceSetup

AlexaForBusinessDeviceSetup 是一项 [AWS 托管策略](#)：提供对 AlexaForBusiness 服务的设备设置权限

使用此策略

您可以将 AlexaForBusinessDeviceSetup 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2019 年 5 月 20 日 21:05 UTC

- ARN: arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessFullAccess

AlexaForBusinessFullAccess 是一项 [AWS 托管策略](#)：授予对 AlexaForBusiness 资源的完全访问权限和对相关 AWS 服务的访问权限

使用此策略

您可以将 AlexaForBusinessFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2020 年 7 月 1 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessGatewayExecution

AlexaForBusinessGatewayExecution 是一项 [AWS 托管策略](#)：提供对 AlexaForBusiness 服务的网关执行权限

使用此策略

您可以将 AlexaForBusinessGatewayExecution 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2017 年 11 月 30 日 16:47 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessLifesizeDelegatedAccessPolicy

AlexaForBusinessLifesizeDelegatedAccessPolicy 是一项 [AWS 托管策略](#)：提供对 Lifesize AVS 设备的访问权限

使用此策略

您可以将 AlexaForBusinessLifesizeDelegatedAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 4 日 19:46 UTC
- 编辑时间：2020 年 6 月 12 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b>DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGWV4TL"
      ]
    }
  ]
}
```



```
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:RegisterAVSDevice"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "a4b:amazonId" : [
          "A2IW07UEGW4TL"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:SearchDevices"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAllValues:StringLike" : {
        "a4b:filters_deviceType" : [
          "*A2IW07UEGW4TL"
        ]
      },
      "Null" : {
        "a4b:filters_deviceType" : "false"
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "a4b:AssociateDeviceWithRoom"
    ],
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A2IW07UEGW4TL",
      "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessNetworkProfileServicePolicy

AlexaForBusinessNetworkProfileServicePolicy 是一项 [AWS 托管策略](#)：此策略允许企业版 Alexa 执行由您的网络配置文件安排的自动化任务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 3 月 13 日 00:53 UTC
- 编辑时间：2019 年 4 月 5 日 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessPolyDelegatedAccessPolicy

AlexaForBusinessPolyDelegatedAccessPolicy 是一项 [AWS 托管策略](#)：提供对 Poly AVS 设备的访问权限

使用此策略

您可以将 AlexaForBusinessPolyDelegatedAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 16 日 19:48 UTC
- 编辑时间：2019 年 10 月 16 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b>DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWW36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWW36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    }
  ],
  {
```

```
    "Action" : [
      "a4b:SearchDevices"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "*"
    ]
  },
  {
    "Action" : [
      "a4b:AssociateDeviceWithRoom"
    ],
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:a4b:us-east-1:*:device/*/*:A238TWW36W3S92",
      "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AlexaForBusinessReadOnlyAccess

AlexaForBusinessReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AlexaForBusiness 服务的只读访问权限

使用此策略

您可以将 AlexaForBusinessReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:47 UTC
- 编辑时间：2019 年 11 月 20 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAPIGatewayAdministrator

AmazonAPIGatewayAdministrator 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 在 Amazon API Gateway 中创建/编辑/删除 API 的完全访问权限。

使用此策略

您可以将 AmazonAPIGatewayAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:34 UTC
- 编辑时间：2015 年 7 月 9 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAPIGatewayInvokeFullAccess

AmazonAPIGatewayInvokeFullAccess 是一项 [AWS 托管策略](#)：提供在 Amazon API Gateway 中调用 API 的完全访问权限。

使用此策略

您可以将 AmazonAPIGatewayInvokeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:36 UTC
- 编辑时间：2018 年 12 月 18 日 18:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAPIGatewayPushToCloudWatchLogs

AmazonAPIGatewayPushToCloudWatchLogs 是一项 [AWS 托管策略](#)：允许 API Gateway 将日志推送到用户的账户。

使用此策略

您可以将 AmazonAPIGatewayPushToCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间 : 2015 年 11 月 11 日 23:41 UTC
- 编辑时间 : 2015 年 11 月 11 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppFlowFullAccess

AmazonAppFlowFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon AppFlow 的完全访问权限，以及对作为流源或目标支持的 AWS 服务（S3 和 Redshift）的访问权限。还提供对 KMS 的访问权限以进行加密。

使用此策略

您可以将 AmazonAppFlowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 2 日 23:30 UTC
- 编辑时间：2022 年 2 月 28 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppFlowReadOnlyAccess

AmazonAppFlowReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon AppFlow 流的只读访问权限

使用此策略

您可以将 AmazonAppFlowReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 2 日 23:26 UTC
- 编辑时间：2022 年 2 月 28 日 20:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppStreamFullAccess

AmazonAppStreamFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon AppStream 的完全访问权限。

使用此策略

您可以将 AmazonAppStreamFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 8 月 28 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppStreamPCAAccess

AmazonAppStreamPCAAccess 是一项 [AWS 托管策略](#)：Amazon AppStream 2.0 访问客户账户中的 AWS Certificate Manager Private CA 以进行基于证书的身份验证

使用此策略

您可以将 AmazonAppStreamPCAAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建日期：2022 年 10 月 24 日 17:05 UTC
- 编辑时间：2022 年 10 月 24 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppStreamReadOnlyAccess

AmazonAppStreamReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon AppStream 的只读访问权限。

使用此策略

您可以将 AmazonAppStreamReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2016 年 12 月 7 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAppStreamServiceAccess

AmazonAppStreamServiceAccess 是一项 [AWS 托管策略](#)：Amazon AppStream 服务角色的默认策略。

使用此策略

您可以将 AmazonAppStreamServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 11 月 19 日 04:17 UTC
- 编辑时间：2020 年 6 月 26 日 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAthenaFullAccess

AmazonAthenaFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Athena 的完全访问权限，以及对启用查询、写入结果和数据管理所需的依赖项的限定访问权限。

使用此策略

您可以将 AmazonAthenaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 16:46 UTC
- 编辑时间：世界标准时间 2024 年 1 月 3 日 19:05
- ARN: arn:aws:iam::aws:policy/AmazonAthenaFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAugmentedAIFullAccess

AmazonAugmentedAIFullAccess 是一项 [AWS 托管策略](#)：提供在 Amazon Augmented AI 资源（包括 FlowDefinitions、HumanTaskUis 和 HumanLoops）上执行所有操作所需的权限。不允许针对 public-crowd Workteam 创建 FlowDefinitions。

使用此策略

您可以将 AmazonAugmentedAIFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:21 UTC
- 编辑时间：2019 年 12 月 3 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAugmentedAIHumanLoopFullAccess

AmazonAugmentedAIHumanLoopFullAccess 是一项 [AWS 托管策略](#)：提供在 HumanLoops 上执行所有操作的权限。

使用此策略

您可以将 AmazonAugmentedAIHumanLoopFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:20 UTC
- 编辑时间：2019 年 12 月 3 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "sagemaker:*HumanLoop",
      "sagemaker:*HumanLoops"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonAugmentedAIIntegratedAPIAccess

AmazonAugmentedAIIntegratedAPIAccess 是一项 [AWS 托管策略](#)：提供在 Amazon Augmented AI 资源（包括 FlowDefinitions、HumanTaskUis 和 HumanLoops）上执行所有操作所需的权限。还提供对与 Amazon Augmented AI 集成的服务的相关操作的访问权限。

使用此策略

您可以将 AmazonAugmentedAIIntegratedAPIAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 22 日 20:47 UTC
- 编辑时间：2020 年 4 月 22 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonBedrockFullAccess

AmazonBedrockFullAccess是一项[AWS托管政策](#)：提供对 Amazon Bedrock 的完全访问权限以及对其所需的相关服务的有限访问权限

使用此策略

您可以将 AmazonBedrockFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 15:47
- 编辑时间：世界标准时间 2023 年 12 月 6 日 15:47
- ARN: arn:aws:iam::aws:policy/AmazonBedrockFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonBedrockReadOnly

AmazonBedrockReadOnly是一项[AWS托管策略](#)，它具有：提供对 Amazon Bedrock 的只读访问权限

使用此策略

您可以将 AmazonBedrockReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 15:48
- 编辑时间：世界标准时间 2023 年 12 月 6 日 15:48
- ARN: arn:aws:iam::aws:policy/AmazonBedrockReadOnly

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonBraketFullAccess

AmazonBraketFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Amazon Braket 的完全访问权限。还提供对相关服务（例如 S3、日志）的访问权限。

使用此策略

您可以将 AmazonBraketFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 6 日 20:12 UTC
- 编辑时间：2023 年 4 月 19 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketFullAccess

策略版本

策略版本：v6（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonBraketJobsExecutionPolicy

AmazonBraketJobsExecutionPolicy 是一项 [AWS 托管策略](#)：授予对 AWS 服务和执行 Amazon Braket Job 所需的资源 (包括 S3、Cloudwatch、IAM 和 Braket) 的访问权限

使用此策略

您可以将 AmazonBraketJobsExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 11 月 26 日 19:34 UTC
- 编辑时间 : 2021 年 11 月 28 日 05:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonBraketServiceRolePolicy

AmazonBraketServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Braket 代表您创建和管理 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 4 日 17:12 UTC
- 编辑时间：2020 年 8 月 6 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeFullAccess

AmazonChimeFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Chime 管理控制台的完全访问权限。

使用此策略

您可以将 AmazonChimeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 1 日 22:15 UTC

- 编辑时间：2020 年 12 月 14 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeReadOnly

AmazonChimeReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Chime 管理控制台的只读访问权限。

使用此策略

您可以将 AmazonChimeReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 1 日 22:04 UTC
- 编辑时间：2020 年 12 月 14 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeReadOnly

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeSDK

AmazonChimeSDK 是一项 [AWS 托管策略](#)：提供对 Amazon Chime SDK 操作的访问权限

使用此策略

您可以将 AmazonChimeSDK 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 2 月 4 日 21:53 UTC
- 编辑时间 : 2023 年 1 月 10 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：适用于 Amazon Chime SDK MediaPipelines 服务关联角色的托管策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 4 月 4 日 22:02 UTC

- 编辑时间：世界标准时间 2023 年 12 月 8 日 19:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeSDKMessagingServiceRolePolicy

AmazonChimeSDKMessagingServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Chime SDK Messaging 访问 AWS 资源并启用消息收发功能

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2023 年 3 月 3 日 01:43 UTC
- 编辑时间：2023 年 3 月 3 日 01:43 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeServiceRolePolicy

AmazonChimeServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 Amazon Chime 使用或管理的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 9 月 30 日 22:25 UTC
- 编辑时间：2019 年 9 月 30 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeTranscriptionServiceLinkedRolePolicy

AmazonChimeTranscriptionServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Chime 代表您访问 Amazon Transcribe 和 Amazon Transcribe Medical

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 4 日 21:47 UTC
- 编辑时间：2021 年 8 月 4 日 21:47 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeUserManagement

AmazonChimeUserManagement 是一项 [AWS 托管策略](#)：通过 AWS Management Console 为用户提供 Amazon Chime 管理控制台的管理权限。

使用此策略

您可以将 AmazonChimeUserManagement 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 1 日 22:17 UTC
- 编辑时间 : 2020 年 2 月 18 日 19:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：适用于 Amazon Chime VoiceConnector 的服务相关角色的托管策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 9 月 30 日 22:16 UTC
- 编辑时间：2023 年 4 月 14 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudDirectoryFullAccess

AmazonCloudDirectoryFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Cloud Directory 服务的完全访问权限。

使用此策略

您可以将 AmazonCloudDirectoryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 25 日 00:41 UTC
- 编辑时间：2017 年 2 月 25 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudDirectoryReadOnlyAccess

AmazonCloudDirectoryReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Cloud Directory 服务的只读访问权限。

使用此策略

您可以将 AmazonCloudDirectoryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 28 日 23:42 UTC
- 编辑时间：2017 年 2 月 28 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchEvidentlyFullAccess

AmazonCloudWatchEvidentlyFullAccess 是一项 [AWS 托管策略](#)：仅提供对 Amazon CloudWatch Evidently 的完全访问权限。还提供对相关 Amazon S3、Amazon SNS、Amazon CloudWatch 和其他相关服务的访问权限。

使用此策略

您可以将 AmazonCloudWatchEvidentlyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 11 月 29 日 15:10 UTC
- 编辑时间 : 2021 年 11 月 29 日 15:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchEvidentlyReadOnlyAccess

AmazonCloudWatchEvidentlyReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CloudWatch Evidently 的只读访问权限

使用此策略

您可以将 AmazonCloudWatchEvidentlyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 15:08 UTC
- 编辑时间：2021 年 11 月 29 日 15:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchEvidentlyServiceRolePolicy

AmazonCloudWatchEvidentlyServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 CloudWatch Evidently Service 代表客户管理相关 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 13 日 17:25 UTC
- 编辑时间：2022 年 9 月 13 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchRUMFullAccess

AmazonCloudWatchRUMFullAccess 是一项 [AWS 托管策略](#)：授予 Amazon CloudWatch RUM 服务的完全访问权限

使用此策略

您可以将 AmazonCloudWatchRUMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 11 月 29 日 15:46 UTC
- 编辑时间 : 2021 年 11 月 29 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchRUMReadOnlyAccess

AmazonCloudWatchRUMReadOnlyAccess 是一项 [AWS 托管策略](#)：授予对 Amazon CloudWatch RUM 服务的只读权限

使用此策略

您可以将 AmazonCloudWatchRUMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 15:43 UTC
- 编辑时间：2022 年 10 月 28 日 18:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCloudWatchRUMServiceRolePolicy

AmazonCloudWatchRUMServiceRolePolicy 是一项 [AWS 托管策略](#)：授予 Amazon CloudWatch RUM 将监控数据发布到其他相关 AWS 服务的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 17 日 23:17 UTC
- 编辑时间：2023 年 2 月 22 日 20:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeCatalystFullAccess

AmazonCodeCatalystFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeCatalyst 的完全访问权限

使用此策略

您可以将 AmazonCodeCatalystFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 4 月 20 日 16:50 UTC
- 编辑时间 : 2023 年 4 月 20 日 16:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    ]
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeCatalystReadOnlyAccess

AmazonCodeCatalystReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeCatalyst 的只读访问权限

使用此策略

您可以将 AmazonCodeCatalystReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 20 日 16:49 UTC
- 编辑时间：2023 年 4 月 20 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeCatalystSupportAccess

AmazonCodeCatalystSupportAccess 是一项 [AWS 托管策略](#)：允许 Amazon CodeCatalyst 代表您创建、更新和解决 AWS Support 案例。

使用此策略

您可以将 AmazonCodeCatalystSupportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 12:34 UTC
- 编辑时间：2023 年 4 月 20 日 12:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruProfilerAgentAccess

AmazonCodeGuruProfilerAgentAccess 是一项 [AWS 托管策略](#)：提供 Amazon CodeGuru Profiler 座席所需的访问权限。

使用此策略

您可以将 AmazonCodeGuruProfilerAgentAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 5 日 22:11 UTC
- 编辑时间：2022 年 5 月 5 日 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruProfilerFullAccess

AmazonCodeGuruProfilerFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeGuru Profiler 的完全访问权限。

使用此策略

您可以将 AmazonCodeGuruProfilerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 10:13 UTC
- 编辑时间：2020 年 7 月 15 日 03:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruProfilerReadOnlyAccess

AmazonCodeGuruProfilerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeGuru Profiler 的只读访问权限。

使用此策略

您可以将 AmazonCodeGuruProfilerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 12 月 3 日 10:30 UTC
- 编辑时间 : 2020 年 6 月 27 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruReviewerFullAccess

AmazonCodeGuruReviewerFullAccess 是一项 [AWS 托管策略](#)：授予对 Amazon CodeGuru Reviewer 的完全访问权限和对所需依赖项的限定访问权限。

使用此策略

您可以将 AmazonCodeGuruReviewerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 08:33 UTC
- 编辑时间：2020 年 8 月 29 日 04:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruReviewerReadOnlyAccess

AmazonCodeGuruReviewerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeGuru Reviewer 的只读访问权限。

使用此策略

您可以将 AmazonCodeGuruReviewerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 08:48 UTC
- 编辑时间：2020 年 8 月 29 日 04:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruReviewerServiceRolePolicy

AmazonCodeGuruReviewerServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon CodeGuru Reviewer 代表您访问资源所需的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 05:31 UTC
- 编辑时间：2020 年 11 月 27 日 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruSecurityFullAccess

AmazonCodeGuruSecurityFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CodeGuru 安全防护工具的完全访问权限。

使用此策略

您可以将 AmazonCodeGuruSecurityFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 9 日 21:03 UTC
- 编辑时间：2023 年 5 月 9 日 21:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCodeGuruSecurityScanAccess

AmazonCodeGuruSecurityScanAccess 是一项 [AWS 托管策略](#)：提供使用 Amazon CodeGuru 安全防御工具扫描所需的访问权限。

使用此策略

您可以将 AmazonCodeGuruSecurityScanAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 5 月 9 日 20:54 UTC
- 编辑时间 : 2023 年 5 月 9 日 20:54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoDeveloperAuthenticatedIdentities

AmazonCognitoDeveloperAuthenticatedIdentities 是一项 [AWS 托管策略](#)：提供对 Amazon Cognito API 的访问权限，以支持开发人员从身份验证后端验证身份。

使用此策略

您可以将 AmazonCognitoDeveloperAuthenticatedIdentities 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 3 月 24 日 17:22 UTC
- 编辑时间：2015 年 3 月 24 日 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoIdpEmailServiceRolePolicy

AmazonCognitoIdpEmailServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Cognito 用户群体服务使用您的 SES 身份发送电子邮件

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 3 月 21 日 21:32 UTC
- 编辑时间：2019 年 3 月 21 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoIdpServiceRolePolicy

AmazonCognitoIdpServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 Amazon Cognito 用户群体使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2020 年 6 月 26 日 22:30 UTC
- 编辑时间：2020 年 6 月 26 日 22:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoPowerUser

AmazonCognitoPowerUser 是一项 [AWS 托管策略](#)：提供对现有 Amazon Cognito 资源的管理访问权限。您需要 AWS 账户管理员权限才能创建新的 Cognito 资源。

使用此策略

您可以将 AmazonCognitoPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 3 月 24 日 17:14 UTC
- 编辑时间 : 2021 年 6 月 1 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoPowerUser

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoReadOnly

AmazonCognitoReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Cognito 资源的只读访问权限。

使用此策略

您可以将 AmazonCognitoReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 3 月 24 日 17:06 UTC
- 编辑时间：2019 年 8 月 1 日 19:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoUnAuthedIdentitiesSessionPolicy

AmazonCognitoUnAuthedIdentitiesSessionPolicy 是一项 [AWS 托管策略](#)：此策略定义了 Cognito 身份池中允许未经验证的身份使用的一组权限。本策略不用作独立的权限策略。它用作一种防护机制，防止对身份池中的角色附加过度宽松的策略。请勿将此策略附加至任何角色，因为 Cognito Identity Service 在创建凭证时会自动将其包含为限定范围的策略。现在，通过增强型流程临时访问其他 AWS 资源的特权将通过以下两部分的交集来定义：服务提供且与未经身份验证用户的身份相关联的角色，以及 Cognito 拥有的此托管策略中给定的特权。

使用此策略

您可以将 AmazonCognitoUnAuthedIdentitiesSessionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 19 日 23:04 UTC
- 编辑时间：2023 年 7 月 19 日 23:04 UTC

- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonCognitoUnauthenticatedIdentities

AmazonCognitoUnauthenticatedIdentities 是一项 [AWS 托管策略](#)：此策略定义了 Cognito 身份池中允许未经身份验证的身份使用的一组权限。无需将其附加到您的未经身份验证的角色，因为 Cognito Identity Service 在创建凭证时会自动将其包含为限定范围的策略。现在，通过增强型流程临时访问其他 AWS 资源的特权将通过以下两部分的交集来定义：服务提供且与未经身份验证用户的身份相关联的角色，以及 Cognito 拥有的此托管策略中给定的特权。

使用此策略

您可以将 AmazonCognitoUnauthenticatedIdentities 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 1 日 22:36 UTC
- 编辑时间：2023 年 2 月 1 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnect_FullAccess

AmazonConnect_FullAccess 是一项 [AWS 托管策略](#)：此策略的目的是向 AWS Connect 用户授予使用 Connect 资源所需的权限。此策略通过 Connect 控制台和公共 API 提供对 AWS Connect 资源的完全访问权限

使用此策略

您可以将 AmazonConnect_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 19:54 UTC
- 编辑时间：2023 年 3 月 7 日 14:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnect_FullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnectCampaignsServiceLinkedRolePolicy

AmazonConnectCampaignsServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：适用于 Amazon Connect 活动服务相关角色的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 23 日 20:54 UTC

- 编辑时间：2023 年 11 月 8 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnectReadOnlyAccess

AmazonConnectReadOnlyAccess 是一项 [AWS 托管策略](#)：授予查看 AWS 账户 中的 Amazon Connect 实例的权限。

使用此策略

您可以将 AmazonConnectReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 17 日 21:00 UTC
- 编辑时间：2019 年 11 月 6 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "Effect" : "Deny",
    "Action" : "connect:GetFederationTokens",
    "Resource" : "*"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnectServiceLinkedRolePolicy

AmazonConnectServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Connect 代表您创建和管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 9 月 7 日 00:21 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 16:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnectSynchronizationServiceRolePolicy

AmazonConnectSynchronizationServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Connect 代表您跨区域同步 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 10 月 27 日 22:38 UTC
- 编辑时间：2023 年 10 月 27 日 22:38 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonConnectVoiceIDFullAccess

AmazonConnectVoiceIDFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Connect Voice ID 的完全访问权限

使用此策略

您可以将 AmazonConnectVoiceIDFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 26 日 19:04 UTC
- 编辑时间：2021 年 9 月 26 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZoneDomainExecutionRolePolicy

AmazonDataZoneDomainExecutionRolePolicy 是一项 [AWS 托管策略](#)：Amazon DomainExecutionRole 服务角色 DataZone 的默认策略。亚马逊使用此角色 DataZone 对亚马逊 DataZone 域中的数据进行分类、发现、管理、共享和分析。

使用此策略

您可以将 AmazonDataZoneDomainExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 27 日 21:55 UTC
- 编辑时间：世界标准时间 2024 年 3 月 12 日 23:48
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneEnvironmentRolePermissionsBoundary

AmazonDataZoneEnvironmentRolePermissionsBoundary 是一项 [AWS 托管策略](#)：Amazon 为环境 DataZone 创建 IAM 角色以执行数据分析操作，并在创建这些角色时使用此策略来定义其权限边界。

使用此策略

您可以将 AmazonDataZoneEnvironmentRolePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 11 日 23:38 UTC
- 编辑时间：世界标准时间 2023 年 11 月 17 日 23:29
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZoneFullAccess

AmazonDataZoneFullAccess 是一项 [AWS 托管策略](#)：DataZone 通过亚马逊提供对亚马逊的完全访问权限，AWS Management Console 以及对亚马逊所需的相关服务的有限访问权限。

使用此策略

您可以将 AmazonDataZoneFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 22 日 20:06 UTC
- 编辑时间：世界标准时间 2024 年 3 月 12 日 16:34
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneFullUserAccess

AmazonDataZoneFullUserAccess 是一项 [AWS 托管策略](#)：提供对 Amazon 的完全访问权限 DataZone，但不允许管理域名、用户或关联账户。

使用此策略

您可以将 AmazonDataZoneFullUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 22 日 21:06 UTC
- 编辑时间：世界标准时间 2024 年 3 月 12 日 23:47
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneGlueManageAccessRolePolicy

AmazonDataZoneGlueManageAccessRolePolicy 是一项 [AWS 托管策略](#)：该策略授予权限以允许 Amazon DataZone 启用数据发布和访问权限。

使用此策略

您可以将 AmazonDataZoneGlueManageAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 22 日 20:21 UTC
- 编辑时间：世界标准时间 2023 年 12 月 14 日 23:03

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

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZonePortalFullAccessPolicy

AmazonDataZonePortalFullAccessPolicy 是一项 [AWS 托管策略](#)：提供对 Amazon DataZone API 的完全访问权限

使用此策略

您可以将 AmazonDataZonePortalFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 26 日 18:24 UTC
- 编辑时间：2023 年 3 月 26 日 18:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZonePreviewConsoleFullAccess

AmazonDataZonePreviewConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon DataZone 预览版的完全访问权限。还提供对其他相关服务的部分访问权限。

使用此策略

您可以将 AmazonDataZonePreviewConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 28 日 15:16 UTC
- 编辑时间：2023 年 7 月 13 日 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZoneProjectDeploymentPermissionsBoundary

AmazonDataZoneProjectDeploymentPermissionsBoundary 是一项 [AWS 托管策略](#)：供 Amazon DataZone 创建用于部署数据分析项目的 IAM 角色。DataZone 在创建这些角色时使用此策略来定义其权限边界。

使用此策略

您可以将 AmazonDataZoneProjectDeploymentPermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 21 日 02:54 UTC
- 编辑时间：2023 年 4 月 4 日 02:48 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonDataZoneProjectDeploymentPermissionsBoundary

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZoneProjectRolePermissionsBoundary

AmazonDataZoneProjectRolePermissionsBoundary 是一项 [AWS 托管策略](#)：Amazon DataZone 为项目创建 IAM 角色以执行数据分析操作，并在创建这些角色时使用此策略来定义其权限边界。

使用此策略

您可以将 AmazonDataZoneProjectRolePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2023 年 3 月 21 日 02:51 UTC
- 编辑时间 : 2023 年 3 月 21 日 02:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicy 是一项 [AWS 托管策略](#)：Amazon DataZone 是一项数据管理服务，可让您对数据进行分类、发现、管理、共享和分析。借助 Amazon DataZone，您可以跨账户和支持的地区共享和访问您的数据。亚马逊 DataZone 简化了您的跨 AWS 服务体验，包括但不限于亚马逊 Redshift、Amazon Athena、Glue 和 Lake Formation。AWS AWS

使用此策略

您可以将 AmazonDataZoneRedshiftGlueProvisioningPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 9 月 22 日 20:19 UTC
- 编辑时间：世界标准时间 2024 年 3 月 12 日 16:44
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonDataZoneRedshiftManageAccessRolePolicy

AmazonDataZoneRedshiftManageAccessRolePolicy 是一项 [AWS 托管策略](#)：该策略授予亚马逊向目录发布亚马逊 Redshift 数据的 DataZone 权限。它还允许亚马逊授予访问 DataZone 权限或撤销对目录中已发布的亚马逊 Redshift 或 Amazon Redshift Serverless 资源的访问权限或撤销访问权限。

使用此策略

您可以将 AmazonDataZoneRedshiftManageAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 9 月 22 日 20:15 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 22:04
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  }
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDetectiveFullAccess

AmazonDetectiveFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Detective 服务的完全访问权限并限定对控制台 UI 依赖项的访问权限

使用此策略

您可以将 AmazonDetectiveFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 30 日 17:57 UTC
- 编辑时间：2023 年 5 月 17 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDetectiveInvestigatorAccess

AmazonDetectiveInvestigatorAccess 是一项 [AWS 托管策略](#)：为调查人员提供对 Amazon Detective 服务的访问权限并限定对控制台 UI 依赖项的访问权限。该策略允许出于调查目的深入探究 Detective，并允许对 Guardduty 的有限写入权限。

使用此策略

您可以将 AmazonDetectiveInvestigatorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 1 月 17 日 15:24 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 27 日 03:13
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDetectiveMemberAccess

AmazonDetectiveMemberAccess 是一项 [AWS 托管策略](#)：为成员提供对 Amazon Detective 服务的访问权限并限定对控制台 UI 依赖项的访问权限。

使用此策略

您可以将 AmazonDetectiveMemberAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 17 日 15:16 UTC
- 编辑时间：2023 年 1 月 17 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDetectiveOrganizationsAccess

AmazonDetectiveOrganizationsAccess 是一项 [AWS 托管策略](#)：为 Organizations 提供管理 Amazon Detective 的委托管理员的访问权限并限定对控制台 UI 依赖项的访问权限。此策略还授予为 Detective 创建服务相关角色的权限。

使用此策略

您可以将 AmazonDetectiveOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 2 日 15:20 UTC

- 编辑时间：2023 年 3 月 2 日 15:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDetectiveServiceLinkedRolePolicy

AmazonDetectiveServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Detective 代表您进行服务调用

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 18 日 19:47 UTC
- 编辑时间：2021 年 11 月 18 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess 是一项 [AWS 托管策略](#)：该策略授予对 DevOps Guru 控制台的完全访问权限。

使用此策略

您可以将 AmazonDevOpsGuruConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 12 月 17 日 18:43 UTC
- 编辑时间：2022 年 8 月 25 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon DevOps Guru 的完全访问权限。

使用此策略

您可以将 AmazonDevOpsGuruFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:38 UTC
- 编辑时间：2022 年 8 月 25 日 18:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruOrganizationsAccess 是一项 [AWS 托管策略](#)：可提供在组织内启用和管理 Amazon DevOps Guru 的权限。

使用此策略

您可以将 AmazonDevOpsGuruOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 15 日 23:50 UTC
- 编辑时间：2021 年 11 月 15 日 23:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess 是一项 [AWS 托管策略](#)：可提供对 Amazon DevOps Guru 控制台的只读访问权限。

使用此策略

您可以将 AmazonDevOpsGuruReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:34 UTC
- 编辑时间：2022 年 8 月 25 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDevOpsGuruServiceRolePolicy

AmazonDevOpsGuruServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon DevOpsGuru 访问您的资源所需的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 1 日 10:24 UTC
- 编辑时间：2023 年 1 月 10 日 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDMSCloudWatchLogsRole

AmazonDMSCloudWatchLogsRole 是一项 [AWS 托管策略](#)：提供将 DMS 复制日志上传到客户账户中的 Cloudwatch 日志的权限。

使用此策略

您可以将 AmazonDMSCloudWatchLogsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 7 日 23:44 UTC
- 编辑时间：2023 年 5 月 23 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    ]
  }
}

```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDMSRedshiftS3Role

AmazonDMSRedshiftS3Role 是一项 [AWS 托管策略](#)：提供管理 DMS 的 Redshift 端点的 S3 设置所需的权限。

使用此策略

您可以将 AmazonDMSRedshiftS3Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 4 月 20 日 17:05 UTC
- 编辑时间：2019 年 7 月 8 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDMSVPCManagementRole

AmazonDMSVPCManagementRole 是一项 [AWS 托管策略](#)：提供管理 AWS 托管客户配置的 VPC 设置所需的权限

使用此策略

您可以将 AmazonDMSVPCManagementRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 18 日 16:33 UTC
- 编辑时间：2016 年 5 月 23 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDB-ElasticServiceRolePolicy

AmazonDocDB-ElasticServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon DocumentDB-Elastic 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建日期：2022 年 11 月 30 日 14:17 UTC
- 编辑时间：2022 年 11 月 30 日 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/DocDB-Elastic"
        ]
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDBConsoleFullAccess

AmazonDocDBConsoleFullAccess 是一项 [AWS 托管策略](#)：提供使用 AWS Management Console 管理 Amazon DocumentDB (与 MongoDB 兼容) 的完全访问权限。请注意，该策略还授予向账户内的所有 SNS 主题发布的完全访问权限、创建和编辑 Amazon EC2 实例和 VPC 配置的权限、在 Amazon KMS 上查看和列出密钥的权限，以及对 Amazon RDS 和 Amazon Neptune 的完全访问权限。

使用此策略

您可以将 AmazonDocDBConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 9 日 20:37 UTC
- 编辑时间：2022 年 11 月 30 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDBElasticFullAccess

AmazonDocDBElasticFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon DocumentDB 弹性集群的完全访问权限及其依赖项（包括 EC2、KMS、SecretsManager、CloudWatch 和 IAM）的其他必需权限。

使用此策略

您可以将 AmazonDocDBElasticFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 5 日 13:51 UTC
- 编辑时间：2023 年 6 月 21 日 18:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDBElasticReadOnlyAccess

AmazonDocDBElasticReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon DocDB-Elastic 和 CloudWatch 指标的只读访问权限。

使用此策略

您可以将 AmazonDocDBElasticReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 8 日 14:37 UTC
- 编辑时间：2023 年 6 月 21 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDBFullAccess

AmazonDocDBFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon DocumentDB (与 MongoDB 兼容) 的完全访问权限。请注意，该策略还授予向账户内的所有 SNS 主题发布的完全访问权限，以及对 Amazon RDS 和 Amazon Neptune 的完全访问权限。

使用此策略

您可以将 AmazonDocDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 1 月 9 日 20:21 UTC
- 编辑时间 : 2019 年 1 月 9 日 20:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:RemoveTagsForResource",
"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"
      }
    }
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDocDBReadOnlyAccess

AmazonDocDBReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon DocumentDB (与 MongoDB 兼容) 的只读访问权限。请注意，该策略还授予对 Amazon RDS 和 Amazon Neptune 资源的访问权限。

使用此策略

您可以将 AmazonDocDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 9 日 20:30 UTC
- 编辑时间：2019 年 1 月 9 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDRSVPCManagement

AmazonDRSVPCManagement 是一项 [AWS 托管策略](#)：提供管理 Amazon 托管客户配置的 VPC 设置的权限

使用此策略

您可以将 AmazonDRSVPCManagement 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 9 月 2 日 00:09 UTC
- 编辑时间 : 2015 年 9 月 2 日 00:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDynamoDBFullAccess

AmazonDynamoDBFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon DynamoDB 的完全访问权限。

使用此策略

您可以将 AmazonDynamoDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2021 年 1 月 29 日 17:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDynamoDBFullAccesswithDataPipeline

AmazonDynamoDBFullAccesswithDataPipeline 是一项 [AWS 托管策略](#)：此策略很快将被弃用。有关指南，请参阅文档：<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html>。提供通过 AWS Management Console 访问 Amazon DynamoDB 的完全访问权限，包括使用 AWS Data Pipeline 进行导出/导入。

使用此策略

您可以将 AmazonDynamoDBFullAccesswithDataPipeline 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2015 年 11 月 12 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonDynamoDBReadOnlyAccess

AmazonDynamoDBReadOnlyAccess 是一项 [AWS 托管策略](#)：通过提供对 Amazon DynamoDB 的只读访问权限。AWS Management Console

使用此策略

您可以将 AmazonDynamoDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 3 月 20 日 15:45
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEBSCSIDriverPolicy

AmazonEBSCSIDriverPolicy 是一项 [AWS 托管策略](#)：允许 CSI 驱动程序服务账户代表您调用 EC2 等相关服务的 IAM policy。

使用此策略

您可以将 AmazonEBSCSIDriverPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 4 日 17:24 UTC
- 编辑时间：2022 年 11 月 18 日 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerRegistryFullAccess

AmazonEC2ContainerRegistryFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ECR 资源的管理访问权限

使用此策略

您可以将 AmazonEC2ContainerRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 21 日 17:06 UTC
- 编辑时间：2020 年 12 月 5 日 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerRegistryPowerUser

AmazonEC2ContainerRegistryPowerUser 是一项 [AWS 托管策略](#)：提供对 Amazon EC2 Container Registry 存储库的完全访问权限，但不允许删除存储库或更改策略。

使用此策略

您可以将 AmazonEC2ContainerRegistryPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 12 月 21 日 17:05 UTC
- 编辑时间 : 2019 年 12 月 10 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerRegistryReadOnly

AmazonEC2ContainerRegistryReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon EC2 Container Registry 存储库的只读访问权限。

使用此策略

您可以将 AmazonEC2ContainerRegistryReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 21 日 17:04 UTC
- 编辑时间：2019 年 12 月 10 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerServiceAutoscaleRole

AmazonEC2ContainerServiceAutoscaleRole 是一项 [AWS 托管策略](#)：用于为 Amazon EC2 Container Service 启用任务自动扩缩的策略

使用此策略

您可以将 AmazonEC2ContainerServiceAutoscaleRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 5 月 12 日 23:25 UTC
- 编辑时间：2018 年 2 月 5 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerServiceEventsRole

AmazonEC2ContainerServiceEventsRole 是一项 [AWS 托管策略](#)：用于为 EC2 Container Service 启用 CloudWatch Events 的策略

使用此策略

您可以将 AmazonEC2ContainerServiceEventsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 5 月 30 日 16:51 UTC
- 编辑时间：2023 年 3 月 6 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerServiceforEC2Role

AmazonEC2ContainerServiceforEC2Role 是一项 [AWS 托管策略](#)：适用于 Amazon EC2 Container Service 的 Amazon EC2 角色的默认策略。

使用此策略

您可以将 AmazonEC2ContainerServiceforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 3 月 19 日 18:45 UTC
- 编辑时间：2023 年 3 月 6 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ContainerServiceRole

AmazonEC2ContainerServiceRole 是一项 [AWS 托管策略](#)：适用于 Amazon ECS 服务角色的默认策略。

使用此策略

您可以将 AmazonEC2ContainerServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 16:14 UTC
- 编辑时间：2016 年 8 月 11 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ]
    }
  ]
}
```



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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2FullAccess

AmazonEC2FullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon EC2 的完全访问权限。

使用此策略

您可以将 AmazonEC2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 11 月 27 日 02:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2ReadOnlyAccess

AmazonEC2ReadOnlyAccess 是一项 [AWS 托管策略](#)：通过提供对 Amazon EC2 的只读访问权限 AWS Management Console。

使用此策略

您可以将 AmazonEC2ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 18:43
- ARN: arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEC2RoleforAWSCodeDeploy

AmazonEC2RoleforAWSCodeDeploy 是一项 [AWS 托管策略](#)：为 S3 桶提供下载修订的 EC2 访问权限。EC2 实例上的 CodeDeploy 座席需要使用此角色。

使用此策略

您可以将 AmazonEC2RoleforAWSCodeDeploy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 19 日 18:10 UTC
- 编辑时间：2017 年 3 月 20 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2RoleforAWSCodeDeployLimited

AmazonEC2RoleforAWSCodeDeployLimited 是一项 [AWS 托管策略](#)：为 S3 桶提供下载修订的 EC2 有限访问权限。EC2 实例上的 CodeDeploy 座席需要使用此角色。

使用此策略

您可以将 AmazonEC2RoleforAWSCodeDeployLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 24 日 17:55 UTC
- 编辑时间：2022 年 1 月 20 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2RoleforDataPipelineRole

AmazonEC2RoleforDataPipelineRole 是一项 [AWS 托管策略](#)：Amazon EC2 Role for Data Pipeline 服务角色的默认策略。

使用此策略

您可以将 AmazonEC2RoleforDataPipelineRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC

- 编辑时间 : 2016 年 2 月 22 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2RoleforSSM

AmazonEC2RoleforSSM 是一项 [AWS 托管策略](#)：此策略很快将被弃用。请使用 AmazonSSMManagedInstanceCore 策略在 EC2 实例上启用 AWS Systems Manager 服务核心功能。有关更多信息，请访问 <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

使用此策略

您可以将 AmazonEC2RoleforSSM 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 29 日 17:48 UTC
- 编辑时间：2019 年 1 月 24 日 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2RolePolicyForLaunchWizard

AmazonEC2RolePolicyForLaunchWizard 是一项 [AWS 托管策略](#)：适用于 EC2 的 Amazon LaunchWizard 服务角色的托管策略

使用此策略

您可以将 AmazonEC2RolePolicyForLaunchWizard 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 08:05 UTC
- 编辑时间：2022 年 5 月 16 日 21:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2SpotFleetAutoscaleRole

AmazonEC2SpotFleetAutoscaleRole 是一项 [AWS 托管策略](#)：用于为 Amazon EC2 竞价型实例集启用自动扩缩的策略

使用此策略

您可以将 AmazonEC2SpotFleetAutoscaleRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 8 月 19 日 18:27 UTC
- 编辑时间：2019 年 2 月 18 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEC2SpotFleetTaggingRole

AmazonEC2SpotFleetTaggingRole 是一项 [AWS 托管策略](#)：允许 EC2 竞价型实例集代表您请求、终止和标记竞价型实例。

使用此策略

您可以将 AmazonEC2SpotFleetTaggingRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 6 月 29 日 18:19 UTC
- 编辑时间：2020 年 4 月 23 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonECS_FullAccess

AmazonECS_FullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ECS 资源的管理访问权限，并通过对其他 AWS 服务资源的访问权限启用 ECS 功能，包括 VPC、自动扩缩组和 CloudFormation 堆栈。

使用此策略

您可以将 AmazonECS_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 7 日 21:36 UTC
- 编辑时间：2023 年 1 月 4 日 16:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECS_FullAccess

策略版本

策略版本：v20 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 是一项 [AWS 托管策略](#)：提供对私有证书颁发机构、Secrets Manager 以及代表您管理 ECS Service Connect TLS 功能 AWS 服务所需的其他内容的管理权限。

使用此策略

您可以将

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 19 日 20:08
- 编辑时间：世界标准时间 2024 年 1 月 19 日 20:08
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AmazonECManaged" : "true",
    "aws:ResourceAccount" : "${aws:PrincipalAccount}"
  }
}
},
{
  "Sid" : "TagOnCreateSecret",
  "Effect" : "Allow",
  "Action" : "secretsmanager:TagResource",
  "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
  "Condition" : {
    "ArnLike" : {
      "aws:RequestTag/AmazonECSCreated" : [
        "arn:aws:ecs:*:*:service/*/*",
        "arn:aws:ecs:*:*:task-set/*/*"
      ]
    },
    "StringEquals" : {
      "aws:RequestTag/AmazonECManaged" : "true",
      "aws:ResourceAccount" : "${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/AmazonECManaged" : "true"
      }
    }
  },
  {
    "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:IssueCertificate"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:ResourceTag/AmazonECManaged" : "true",
        "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonECSInfrastructureRolePolicyForVolumes

AmazonECSInfrastructureRolePolicyForVolumes 是一项 [AWS 托管策略](#)：提供代表您管理与 ECS 工作负载关联的卷所需的其他 AWS 服务资源的访问权限。

使用此策略

您可以将 AmazonECSInfrastructureRolePolicyForVolumes 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 10 日 22:56
- 编辑时间：世界标准时间 2024 年 1 月 10 日 22:56
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AmazonECSManaged" : "arn:aws:ecs:*:*:task/*"
      },
      "StringEquals" : {
        "aws:ResourceTag/AmazonECSManaged" : "true"
      }
    }
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonECSServiceRolePolicy

AmazonECSServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon ECS 管理您的集群的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 14 日 01:18 UTC
- 编辑时间：世界标准时间 2023 年 12 月 4 日 19:32
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AmazonEC2Managed" : "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonECSTaskExecutionRolePolicy

AmazonECSTaskExecutionRolePolicy 是一项 [AWS 托管策略](#)：提供对运行 Amazon ECS 任务所必需的其他 AWS 服务资源的访问权限

使用此策略

您可以将 AmazonECSTaskExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 16 日 18:48 UTC
- 编辑时间：2017 年 11 月 16 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEFSCSIDriverPolicy

AmazonEFSCSIDriverPolicy 是一项 [AWS 托管策略](#)：提供对 EFS 资源的管理访问权限和 EC2 的读取访问权限

使用此策略

您可以将 AmazonEFSCSIDriverPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 7 月 25 日 20:10 UTC
- 编辑时间：2023 年 7 月 25 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKS_CNI_Policy

AmazonEKS_CNI_Policy 是一项 [AWS 托管策略](#)：此策略为 Amazon VPC CNI 插件 (amazon-vpc-cni-k8s) 提供了修改您的 EKS 工作节点上的 IP 地址配置所需的权限。此权限集允许 CNI 代表您列出、描述和修改弹性网络接口。有关 AWS VPC CNI 插件的更多信息，请点击此处：<https://github.com/aws/8s-amazon-vpc-cni-k>

使用此策略

您可以将 AmazonEKS_CNI_Policy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 27 日 21:07 UTC
- 编辑时间：世界标准时间 2024 年 3 月 4 日 20:20
- ARN: arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonEKSClusterPolicy

AmazonEKSClusterPolicy 是一项 [AWS 托管策略](#)：此策略为 Kubernetes 提供代表您管理资源所需的权限。Kubernetes 需要 `Ec2:CreateTags` 权限才能在 EC2 资源（包括但不限于实例、安全组和弹性网络接口）上放置识别信息。

使用此策略

您可以将 AmazonEKSClusterPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 5 月 27 日 21:06 UTC
- 编辑时间 : 2023 年 2 月 7 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSCoordinatorServiceRolePolicy

AmazonEKSCoordinatorServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略允许 Amazon EKS 管理 EKS 连接器的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 4 日 20:31 UTC
- 编辑时间：2021 年 9 月 4 日 20:31 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSFargatePodExecutionRolePolicy

AmazonEKSFargatePodExecutionRolePolicy 是一项 [AWS 托管策略](#)：提供对在 AWS Fargate 上运行 Amazon EKS 容器组 (pod) 所必需的其他 AWS 服务资源的访问权限

使用此策略

您可以将 AmazonEKSFargatePodExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 22 日 04:34 UTC
- 编辑时间：2019 年 11 月 22 日 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSFargateServiceRolePolicy

AmazonEKSFargateServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略授予 Amazon EKS 运行 Fargate 任务必需的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 22 日 04:36 UTC
- 编辑时间：2019 年 11 月 22 日 04:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSFargateServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSLocalOutpostClusterPolicy

AmazonEKSLocalOutpostClusterPolicy 是一项 [AWS 托管策略](#)：此策略为在您的账户中运行的 EKS 本地集群控制面板实例提供代表您管理资源的权限。

使用此策略

您可以将 AmazonEKSLocalOutpostClusterPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 8 月 24 日 21:56 UTC
- 编辑时间 : 2022 年 10 月 17 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSLocalOutpostServiceRolePolicy

AmazonEKSLocalOutpostServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon EKS Local 代表您调用 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 8 月 23 日 21:53 UTC
- 编辑时间：2022 年 10 月 24 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSServicePolicy

AmazonEKSServicePolicy 是一项 [AWS 托管策略](#)：此策略允许 Amazon Elastic Container Service for Kubernetes 创建和管理运行 EKS 集群所需的资源。

使用此策略

您可以将 AmazonEKSServicePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2018 年 5 月 27 日 21:08 UTC
- 编辑时间 : 2020 年 5 月 27 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSServiceRolePolicy

AmazonEKSServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon EKS 需要服务相关角色才能代表您调用 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 2 月 21 日 20:10 UTC
- 编辑时间：2020 年 5 月 27 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSVPCResourceController

AmazonEKSVPCResourceController 是一项 [AWS 托管策略](#)：VPC 资源控制器用于管理 Worker 节点的 ENI 和 IP 的策略。

使用此策略

您可以将 AmazonEKSVPCResourceController 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 12 日 00:55 UTC
- 编辑时间：2020 年 8 月 12 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEKSWorkerNodePolicy

AmazonEKSWorkerNodePolicy 是一项 [AWS 托管策略](#)：此策略允许 Amazon EKS Worker 节点连接到 Amazon EKS 集群。

使用此策略

您可以将 AmazonEKSWorkerNodePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 5 月 27 日 21:09 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 00:06
- ARN: arn:aws:iam::aws:policy/AmazonEKSEKSWorkerNodePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElastiCacheFullAccess

AmazonElastiCacheFullAccess 是一项 [AWS 托管策略](#)：提供 ElastiCache 通过 Amazon 的完全访问权限 AWS Management Console。

使用此策略

您可以将 AmazonElastiCacheFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 03:49
- ARN: arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticCacheReadOnlyAccess

AmazonElasticCacheReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon ElasticCache 的只读访问权限。

使用此策略

您可以将 AmazonElasticCacheReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticCacheReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  ]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticContainerRegistryPublicFullAccess

AmazonElasticContainerRegistryPublicFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ECR Public 资源的管理访问权限

使用此策略

您可以将 AmazonElasticContainerRegistryPublicFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 17:25 UTC
- 编辑时间：2020 年 12 月 1 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonElasticContainerRegistryPublicFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticContainerRegistryPublicPowerUser

AmazonElasticContainerRegistryPublicPowerUser 是一项 [AWS 托管策略](#)：提供对 Amazon ECR Public 存储库的完全访问权限，但不允许删除存储库或更改策略。

使用此策略

您可以将 AmazonElasticContainerRegistryPublicPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:16 UTC
- 编辑时间：2020 年 12 月 1 日 16:16 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticContainerRegistryPublicReadOnly

AmazonElasticContainerRegistryPublicReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon ECR Public 存储库的只读访问权限。

使用此策略

您可以将 AmazonElasticContainerRegistryPublicReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 17:27 UTC
- 编辑时间：2020 年 12 月 1 日 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemClientFullAccess

AmazonElasticFileSystemClientFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EFS 文件系统的根客户端访问权限

使用此策略

您可以将 AmazonElasticFileSystemClientFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 13 日 16:27 UTC
- 编辑时间：2020 年 1 月 13 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemClientReadOnlyAccess

AmazonElasticFileSystemClientReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EFS 文件系统的只读客户端访问权限

使用此策略

您可以将 AmazonElasticFileSystemClientReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 1 月 13 日 16:24 UTC
- 编辑时间 : 2020 年 1 月 13 日 16:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemClientReadWriteAccess

AmazonElasticFileSystemClientReadWriteAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EFS 文件系统的读取和写入客户端访问权限

使用此策略

您可以将 AmazonElasticFileSystemClientReadWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 13 日 16:21 UTC
- 编辑时间：2020 年 1 月 13 日 16:21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ]
    }
  ]
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemFullAccess

AmazonElasticFileSystemFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon EFS 的完全访问权限。

使用此策略

您可以将 AmazonElasticFileSystemFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 27 日 16:22 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 16:53
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemReadOnlyAccess

AmazonElasticFileSystemReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon EFS 的只读访问权限。

使用此策略

您可以将 AmazonElasticFileSystemReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 27 日 16:25 UTC
- 编辑时间：2022 年 1 月 10 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemServiceRolePolicy

AmazonElasticFileSystemServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Elastic File System 代表您管理 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 5 日 16:52 UTC
- 编辑时间：2022 年 1 月 10 日 19:27 UTC

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

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticFileSystemsUtils

AmazonElasticFileSystemsUtils 是一项 [AWS 托管策略](#)：允许客户使用 AWS Systems Manager 自动管理其 EC2 实例上的 Amazon EFS 实用程序 (amazon-efs-utils) 软件包，并使用 CloudWatchLog 获取 EFS 文件系统挂载成功/失败通知。

使用此策略

您可以将 AmazonElasticFileSystemsUtils 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 29 日 15:16 UTC
- 编辑时间：2020 年 9 月 29 日 15:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceEditorsRole

AmazonElasticMapReduceEditorsRole 是一项 [AWS 托管策略](#)：Amazon Elastic MapReduce Editors 服务角色的默认策略。

使用此策略

您可以将 AmazonElasticMapReduceEditorsRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 16 日 21:55 UTC
- 编辑时间：2023 年 2 月 9 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceforAutoScalingRole

AmazonElasticMapReduceforAutoScalingRole 是一项 [AWS 托管策略](#)：Amazon Elastic MapReduce for Auto Scaling。允许 Auto Scaling 向您的 EMR 集群中添加和从中删除实例的角色。

使用此策略

您可以将 AmazonElasticMapReduceforAutoScalingRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 11 月 18 日 01:09 UTC
- 编辑时间：2016 年 11 月 18 日 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceforEC2Role

AmazonElasticMapReduceforEC2Role 是一项 [AWS 托管策略](#)：Amazon Elastic MapReduce for EC2 服务角色的默认策略。

使用此策略

您可以将 AmazonElasticMapReduceforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2017 年 8 月 11 日 23:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceFullAccess

AmazonElasticMapReduceFullAccess 是一项 [AWS 托管策略](#)：此策略很快将被弃用。有关指南，请参阅文档：<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。提供对 Amazon Elastic MapReduce 及其所需的底层服务（例如 EC2 和 S3）的完全访问权限

使用此策略

您可以将 AmazonElasticMapReduceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 10 月 11 日 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReducePlacementGroupPolicy

AmazonElasticMapReducePlacementGroupPolicy 是一项 [AWS 托管策略](#)：允许 EMR 创建、描述和删除 EC2 置放组的策略。

使用此策略

您可以将 AmazonElasticMapReducePlacementGroupPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 29 日 00:37 UTC
- 编辑时间：2020 年 9 月 29 日 00:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceReadOnlyAccess

AmazonElasticMapReduceReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Elastic MapReduce 的只读访问权限。

使用此策略

您可以将 AmazonElasticMapReduceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 7 月 29 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticMapReduceRole

AmazonElasticMapReduceRole 是一项 [AWS 托管策略](#)：此策略很快将被弃用。有关指南，请参阅文档：<https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html>。Amazon Elastic MapReduce 服务角色的默认策略。

使用此策略

您可以将 AmazonElasticMapReduceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2020 年 6 月 24 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticsearchServiceRolePolicy

AmazonElasticsearchServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Elasticsearch Service 代表您访问其他 AWS 服务，例如 EC2 网络 API。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2017 年 7 月 7 日 00:15 UTC
- 编辑时间 : 2023 年 10 月 23 日 06:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticTranscoder_FullAccess

AmazonElasticTranscoder_FullAccess 是一项 [AWS 托管策略](#)：向用户授予对 Elastic Transcoder 的完全访问权限以及使用 Elastic Transcoder 完整功能所需的相关服务的访问权限。

使用此策略

您可以将 AmazonElasticTranscoder_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 27 日 18:59 UTC
- 编辑时间：2019 年 6 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticTranscoder_JobsSubmitter

AmazonElasticTranscoder_JobsSubmitter 是一项 [AWS 托管策略](#)：授予用户更改预设、提交作业和查看 Elastic Transcoder 设置的权限。此策略还授予使用 Elastic Transcoder 控制台所需的某些其他服务的某些只读访问权限，包括 S3、IAM 和 SNS。

使用此策略

您可以将 AmazonElasticTranscoder_JobsSubmitter 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 6 月 7 日 21:12 UTC
- 编辑时间 : 2019 年 6 月 10 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticTranscoder_ReadOnlyAccess

AmazonElasticTranscoder_ReadOnlyAccess 是一项 [AWS 托管策略](#)：授予用户对 Elastic Transcoder 的只读访问权限和对相关服务的列表访问权限。

使用此策略

您可以将 AmazonElasticTranscoder_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 7 日 21:09 UTC
- 编辑时间：2019 年 6 月 10 日 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
{
  "Action" : [
    "elastictranscoder:Read*",
    "elastictranscoder:List*",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "iam:ListRoles",
    "sns:ListTopics"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonElasticTranscoderRole

AmazonElasticTranscoderRole 是一项 [AWS 托管策略](#)：Amazon Elastic Transcoder 服务角色的默认策略。

使用此策略

您可以将 AmazonElasticTranscoderRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2019 年 6 月 13 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRCleanupPolicy

AmazonEMRCleanupPolicy 是一项 [AWS 托管策略](#)：允许 EMR 在 EMR 服务角色失去终止和删除 AWS EC2 资源所需的能力时执行这些操作。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 26 日 23:54 UTC
- 编辑时间：2020 年 9 月 29 日 21:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRContainersServiceRolePolicy

AmazonEMRContainersServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问运行 Amazon EMR 必需的其他 AWS 服务资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 9 日 00:38 UTC
- 编辑时间：2023 年 3 月 10 日 22:58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRFullAccessPolicy_v2

AmazonEMRFullAccessPolicy_v2 是一项 [AWS 托管策略](#)：提供对 Amazon EMR 的完全访问权限

使用此策略

您可以将 AmazonEMRFullAccessPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 12 日 01:50 UTC
- 编辑时间：2023 年 7 月 28 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRReadOnlyAccessPolicy_v2

AmazonEMRReadOnlyAccessPolicy_v2 是一项 [AWS 托管策略](#)：提供对 Amazon EMR 和相关 CloudWatch 指标的只读访问权限。

使用此策略

您可以将 AmazonEMRReadOnlyAccessPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 12 日 01:39 UTC
- 编辑时间：2023 年 8 月 2 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRServerlessServiceRolePolicy

AmazonEMRServerlessServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问运行 Amazon EMRServerless 必需的其他 AWS 服务资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 5 月 20 日 23:15 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 18:21
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEMRServicePolicy_v2

AmazonEMRServicePolicy_v2 是一项 [AWS 托管策略](#)：此策略用于 Amazon EMR 服务角色，不得用于您账户中的任何其他 IAM 用户或角色。此策略授予创建和管理 EMR 相关资源以及运行 EMR 集群所需的相关服务的权限。

使用此策略

您可以将 AmazonEMRServicePolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 3 月 12 日 01:11 UTC
- 编辑时间：2022 年 2 月 15 日 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonESCognitoAccess

AmazonESCognitoAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Cognito 配置服务的有限访问权限。

使用此策略

您可以将 AmazonESCognitoAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 28 日 22:29 UTC
- 编辑时间：2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESCognitoAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonESFullAccess

AmazonESFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ES 配置服务的完全访问权限。

使用此策略

您可以将 AmazonESFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 1 日 19:14 UTC
- 编辑时间：2015 年 10 月 1 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonESReadOnlyAccess

AmazonESReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ES 配置服务的只读访问权限。

使用此策略

您可以将 AmazonESReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 1 日 19:18 UTC
- 编辑时间：2018 年 10 月 3 日 03:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeApiDestinationsServiceRolePolicy

AmazonEventBridgeApiDestinationsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 EventBridge 代表您访问 Secret Manager 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 2 月 11 日 20:52 UTC
- 编辑时间：2021 年 2 月 11 日 20:52 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeFullAccess

AmazonEventBridgeFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge 的完全访问权限。

使用此策略

您可以将 AmazonEventBridgeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 7 月 11 日 14:08 UTC
- 编辑时间 : 2022 年 12 月 1 日 17:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgePipesFullAccess

AmazonEventBridgePipesFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge Pipes 的完全访问权限。

使用此策略

您可以将 AmazonEventBridgePipesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 12 月 1 日 17:03 UTC
- 编辑时间 : 2022 年 12 月 1 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgePipesOperatorAccess

AmazonEventBridgePipesOperatorAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge Pipes 的只读访问权限和操作员（能够停止和开始运行 Pipes）访问权限。

使用此策略

您可以将 AmazonEventBridgePipesOperatorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 12 月 1 日 17:04 UTC
- 编辑时间：2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    "Action" : [
      "pipes:DescribePipe",
      "pipes:ListPipes",
      "pipes:ListTagsForResource",
      "pipes:StartPipe",
      "pipes:StopPipe"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgePipesReadOnlyAccess

AmazonEventBridgePipesReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge Pipes 的只读访问权限。

使用此策略

您可以将 AmazonEventBridgePipesReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 12 月 1 日 17:04 UTC
- 编辑时间：2022 年 12 月 1 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeReadOnlyAccess

AmazonEventBridgeReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge 的只读访问权限。

使用此策略

您可以将 AmazonEventBridgeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2019 年 7 月 11 日 13:59 UTC
- 编辑时间 : 2022 年 12 月 1 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeSchedulerFullAccess

AmazonEventBridgeSchedulerFullAccess 是一项 [AWS 托管策略](#)：

AmazonEventBridgeSchedulerFullAccess 托管策略为调度和调度组授予使用所有 EventBridge 调度器操作的权限。

使用此策略

您可以将 AmazonEventBridgeSchedulerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 11 月 10 日 18:37 UTC
- 编辑时间 : 2022 年 11 月 10 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeSchedulerReadOnlyAccess

AmazonEventBridgeSchedulerReadOnlyAccess 是一项 [AWS 托管策略](#)：

AmazonEventBridgeSchedulerReadOnlyAccess 托管策略授予查看有关调度和调度组的详细信息的只读权限

使用此策略

您可以将 AmazonEventBridgeSchedulerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 18:50 UTC
- 编辑时间：2022 年 11 月 10 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "scheduler:ListSchedules",
      "scheduler:ListScheduleGroups",
      "scheduler:GetSchedule",
      "scheduler:GetScheduleGroup",
      "scheduler:ListTagsForResource"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeSchemasFullAccess

AmazonEventBridgeSchemasFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge Schemas 的完全访问权限。

使用此策略

您可以将 AmazonEventBridgeSchemasFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 28 日 23:12 UTC
- 编辑时间：2019 年 11 月 28 日 23:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeSchemasReadOnlyAccess

AmazonEventBridgeSchemasReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon EventBridge Schemas 的只读访问权限。

使用此策略

您可以将 AmazonEventBridgeSchemasReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 28 日 23:05 UTC
- 编辑时间：2020 年 5 月 1 日 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonEventBridgeSchemasServiceRolePolicy

AmazonEventBridgeSchemasServiceRolePolicy 是一项 [AWS 托管策略](#)：向由 Amazon EventBridge 架构创建的托管规则授予权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2019 年 11 月 27 日 01:10 UTC
- 编辑时间 : 2019 年 11 月 27 日 01:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFISServiceRolePolicy

AmazonFISServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS FIS 管理实验监控和资源选择的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 21 日 21:18 UTC
- 编辑时间：2022 年 10 月 25 日 09:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonForecastFullAccess

AmazonForecastFullAccess 是一项 [AWS 托管策略](#)：允许访问 Amazon Forecast 的所有操作

使用此策略

您可以将 AmazonForecastFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 01:52 UTC
- 编辑时间：2019 年 1 月 18 日 01:52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "forecast:*"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : "forecast.amazonaws.com"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFraudDetectorFullAccessPolicy

AmazonFraudDetectorFullAccessPolicy 是一项 [AWS 托管策略](#)：允许访问 Amazon Fraud Detector 的所有操作

使用此策略

您可以将 AmazonFraudDetectorFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 12 月 3 日 22:46 UTC
- 编辑时间 : 2019 年 12 月 3 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFreeRTOSFullAccess

AmazonFreeRTOSFullAccess 是一项 [AWS 托管策略](#) : Amazon FreeRTOS 的完全访问策略

使用此策略

您可以将 AmazonFreeRTOSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 29 日 15:32 UTC
- 编辑时间 : 2017 年 11 月 29 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFreeRTOSOTAUpdate

AmazonFreeRTOSOTAUpdate 是一项 [AWS 托管策略](#)：允许用户访问 Amazon FreeRTOS OTA 更新

使用此策略

您可以将 AmazonFreeRTOSOTAUpdate 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 8 月 27 日 22:43 UTC
- 编辑时间：2020 年 12 月 18 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFSxConsoleFullAccess

AmazonFSxConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon FSx 的完全访问权限和对 AWS 相关服务的访问权限。

使用此策略

您可以将 AmazonFSxConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:36 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:07
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    ]
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFSxConsoleReadOnlyAccess

AmazonFSxConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon FSx 的只读访问权限和对 AWS 相关服务的访问权限。

使用此策略

您可以将 AmazonFSxConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:35 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:19
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFSxFullAccess

AmazonFSxFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon FSx 的完全访问权限和对相关 AWS 服务的访问权限。

使用此策略

您可以将 AmazonFSxFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 16:34 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:16
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFSxReadOnlyAccess

AmazonFSxReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon FSx 的只读访问权限。

使用此策略

您可以将 AmazonFSxReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 11 月 28 日 16:33 UTC
- 编辑时间：2018 年 11 月 28 日 16:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonFSxServiceRolePolicy

AmazonFSxServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon FSx 代表您管理 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 28 日 10:38 UTC
- 编辑时间：世界标准时间 2024 年 1 月 10 日 20:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGlacierFullAccess

AmazonGlacierFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Glacier 的完全访问权限。

使用此策略

您可以将 AmazonGlacierFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGlacierReadOnlyAccess

AmazonGlacierReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Glacier 的只读访问权限。

使用此策略

您可以将 AmazonGlacierReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2016 年 5 月 5 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGrafanaAthenaAccess

AmazonGrafanaAthenaAccess 是一项 [AWS 托管策略](#)：此策略授予访问 Amazon Athena 和所需依赖项的权限，以便能够通过 Amazon Grafana 中的 Amazon Athena 插件查询结果并将结果写入 s3。

使用此策略

您可以将 AmazonGrafanaAthenaAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 22 日 17:11 UTC
- 编辑时间：2021 年 11 月 22 日 17:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGrafanaCloudWatchAccess

AmazonGrafanaCloudWatchAccess 是一项 [AWS 托管策略](#)：此策略授予访问 Amazon CloudWatch，以及在 Amazon Managed Grafana 中使用 CloudWatch 作为数据源所需的依赖项的权限。

使用此策略

您可以将 AmazonGrafanaCloudWatchAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 3 月 24 日 22:41 UTC
- 编辑时间：2023 年 3 月 24 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGrafanaRedshiftAccess

AmazonGrafanaRedshiftAccess 是一项 [AWS 托管策略](#)：此策略授予对 Amazon Redshift，以及在 Amazon Grafana 中使用 Amazon Redshift 插件所需的依赖项的限定访问权限。

使用此策略

您可以将 AmazonGrafanaRedshiftAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 26 日 23:15 UTC

- 编辑时间：2021 年 11 月 26 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGrafanaServiceLinkedRolePolicy

AmazonGrafanaServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：提供对 Amazon Grafana 管理或使用的 AWS 资源的访问权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2022 年 11 月 8 日 23:10 UTC
- 编辑时间：2022 年 11 月 8 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGuardDutyFullAccess

AmazonGuardDutyFullAccess是一项[AWS托管策略](#)：提供使用 Amazon 的完全访问权限 GuardDuty。

使用此策略

您可以将 AmazonGuardDutyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 28 日 22:31 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 16 日 23:04
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGuardDutyMalwareProtectionServiceRolePolicy

AmazonGuardDutyMalwareProtectionServiceRolePolicy 是一

种 [AWS 托管策略](#)：GuardDuty 恶意软件防护使用名为的服务相关角色 (SLR)。

AWSServiceRoleForAmazonGuardDutyMalwareProtection 此服务相关角色允许 GuardDuty 恶意软件防护执行无代理扫描以检测恶意软件。它 GuardDuty 允许在您的帐户中创建快照，并与 GuardDuty 服务帐户共享快照以扫描恶意软件。它会评估这些共享快照，并将检索到的 EC2 实例元数据包含在 GuardDuty 恶意软件防护结果中。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服务相关角色信任恶意软件保护.guardduty.amazonaws.com 服务来代替该角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 19 日 19:06 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 22:24
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGuardDutyReadOnlyAccess

AmazonGuardDutyReadOnlyAccess是一项[AWS托管策略](#)，它：提供对 Amazon GuardDuty 资源的只读访问权限

使用此策略

您可以将 AmazonGuardDutyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 22:29 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 23:07
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonGuardDutyServiceRolePolicy

AmazonGuardDutyServiceRolePolicy是一项[AWS 托管策略](#)：允许访问由 Amazon Guard Duty 使用或管理的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 28 日 20:12 UTC
- 编辑时间：世界标准时间 2024 年 2 月 9 日 18:30
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonHealthLakeFullAccess

AmazonHealthLakeFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon HealthLake 服务的完全访问权限。

使用此策略

您可以将 AmazonHealthLakeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 01:07 UTC
- 编辑时间：2021 年 2 月 17 日 01:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHealthLakeReadOnlyAccess

AmazonHealthLakeReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon HealthLake 服务的只读访问权限。

使用此策略

您可以将 AmazonHealthLakeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 02:43 UTC
- 编辑时间：2021 年 2 月 17 日 02:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeFullAccess

AmazonHoneycodeFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode 的完全访问权限。

使用此策略

您可以将 AmazonHoneycodeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeReadOnlyAccess

AmazonHoneycodeReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode 的只读访问权限。

使用此策略

您可以将 AmazonHoneycodeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
      ],
    },
  ],
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeServiceRolePolicy

AmazonHoneycodeServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon Honeycode 访问您的资源所需的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 18 日 18:03 UTC
- 编辑时间：2020 年 11 月 18 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeTeamAssociationFullAccess

AmazonHoneycodeTeamAssociationFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode Team Association 的完全访问权限。

使用此策略

您可以将 AmazonHoneycodeTeamAssociationFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 6 月 24 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeTeamAssociationReadOnlyAccess

AmazonHoneycodeTeamAssociationReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode Team Association 的只读访问权限。

使用此策略

您可以将 AmazonHoneycodeTeamAssociationReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 6 月 24 日 20:27 UTC
- 编辑时间 : 2020 年 6 月 24 日 20:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeWorkbookFullAccess

AmazonHoneycodeWorkbookFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode Workbook 的完全访问权限。

使用此策略

您可以将 AmazonHoneycodeWorkbookFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonHoneycodeWorkbookReadOnlyAccess

AmazonHoneycodeWorkbookReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Honeycode Workbook 的只读访问权限。

使用此策略

您可以将 AmazonHoneycodeWorkbookReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 20:28 UTC
- 编辑时间：2020 年 12 月 1 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspector2AgentlessServiceRolePolicy

AmazonInspector2AgentlessServiceRolePolicy是一项[AWS托管策略](#)，它：向 Amazon Inspector 授予执行无代理安全评估AWS 服务所需的访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：世界标准时间 2023 年 11 月 20 日 15:18
- 编辑时间：世界标准时间 2023 年 11 月 20 日 15:18
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspector2FullAccess

AmazonInspector2FullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Inspector 的完全访问权限以及对其他相关服务（例如 Organizations）的访问权限。

使用此策略

您可以将 AmazonInspector2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 19:10 UTC
- 编辑时间：2023 年 8 月 3 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

策略版本

策略版本：v3（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspector2ManagedCisPolicy

AmazonInspector2ManagedCisPolicy 是一项 [AWS 托管策略](#)：这是一项托管策略，客户应将其附加到自己的角色上，以便与检查员服务部门进行通信以进行 CIS 扫描

使用此策略

您可以将 AmazonInspector2ManagedCisPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 世界标准时间 2024 年 1 月 24 日 16:31
- 编辑时间 : 世界标准时间 2024 年 1 月 24 日 16:31
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspector2ReadOnlyAccess

AmazonInspector2ReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon inspector2 服务和相关支持服务的只读访问权限

使用此策略

您可以将 AmazonInspector2ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 1 月 21 日 14:45 UTC
- 编辑时间：2023 年 9 月 22 日，20:56 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspector2ServiceRolePolicy

AmazonInspector2ServiceRolePolicy 是一项 [AWS 托管策略](#)：向 Amazon Inspector 授予执行安全评测所需的 AWS 服务访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 16 日 20:27 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 14:06
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy

策略版本

策略版本 : v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspectorFullAccess

AmazonInspectorFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Inspector 的完全访问权限。

使用此策略

您可以将 AmazonInspectorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 17:08 UTC

- 编辑时间：2017 年 12 月 21 日，14:53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspectorReadOnlyAccess

AmazonInspectorReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Inspector 的只读访问权限。

使用此策略

您可以将 AmazonInspectorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 17:08 UTC
- 编辑时间：2019 年 10 月 1 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

策略版本

策略版本：v4（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonInspectorServiceRolePolicy

AmazonInspectorServiceRolePolicy 是一项 [AWS 托管策略](#)：向 Amazon Inspector 授予执行安全评测所需的 AWS 服务访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 21 日 15:48 UTC
- 编辑时间：2020 年 9 月 11 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKendraFullAccess

AmazonKendraFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Kendra 的完全访问权限。

使用此策略

您可以将 AmazonKendraFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 16:15 UTC
- 编辑时间：2019 年 12 月 3 日 16:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKendraReadOnlyAccess

AmazonKendraReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Kendra 的只读访问权限。

使用此策略

您可以将 AmazonKendraReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2019 年 12 月 3 日 16:13 UTC
- 编辑时间：2021 年 5 月 27 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKeyspacesFullAccess

AmazonKeyspacesFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Keyspaces 的完全访问权限

使用此策略

您可以将 AmazonKeyspacesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 23 日 17:06 UTC
- 编辑时间：2023 年 10 月 3 日，19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKeyspacesReadOnlyAccess

AmazonKeyspacesReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Keyspaces 的只读访问权限

使用此策略

您可以将 AmazonKeyspacesReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 23 日 17:07 UTC
- 编辑时间：2022 年 7 月 7 日 14:54 UTC

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

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKeyspacesReadOnlyAccess_v2

AmazonKeyspacesReadOnlyAccess_v2 是一项 [AWS 托管策略](#)：提供对 Amazon Keyspaces 和相关 AWS 服务的只读访问权限。

使用此策略

您可以将 AmazonKeyspacesReadOnlyAccess_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 12 日 17:01 UTC
- 编辑时间：2023 年 9 月 12 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisAnalyticsFullAccess

AmazonKinesisAnalyticsFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Kinesis Analytics 的完全访问权限。

使用此策略

您可以将 AmazonKinesisAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 9 月 21 日 19:01 UTC
- 编辑时间 : 2016 年 9 月 21 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisAnalyticsReadOnly

AmazonKinesisAnalyticsReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Kinesis Analytics 的只读访问权限。

使用此策略

您可以将 AmazonKinesisAnalyticsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 9 月 21 日 18:16 UTC
- 编辑时间：2016 年 9 月 21 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisFirehoseFullAccess

AmazonKinesisFirehoseFullAccess 是一项 [AWS 托管策略](#)：提供对所有 Amazon Kinesis Firehose Delivery Streams 的完全访问权限。

使用此策略

您可以将 AmazonKinesisFirehoseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 18:45 UTC
- 编辑时间：2015 年 10 月 7 日 18:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisFirehoseReadOnlyAccess

AmazonKinesisFirehoseReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 Amazon Kinesis Firehose Delivery Streams 的只读访问权限。

使用此策略

您可以将 AmazonKinesisFirehoseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 7 日 18:43 UTC
- 编辑时间：2015 年 10 月 7 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisFullAccess

AmazonKinesisFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有流的完全访问权限。

使用此策略

您可以将 AmazonKinesisFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisReadOnlyAccess

AmazonKinesisReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有流的只读访问权限。

使用此策略

您可以将 AmazonKinesisReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisVideoStreamsFullAccess

AmazonKinesisVideoStreamsFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Kinesis Video Streams 的完全访问权限。

使用此策略

您可以将 AmazonKinesisVideoStreamsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 1 日 23:27 UTC
- 编辑时间：2017 年 12 月 1 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonKinesisVideoStreamsReadOnlyAccess

AmazonKinesisVideoStreamsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Kinesis Video Streams 的只读访问权限。

使用此策略

您可以将 AmazonKinesisVideoStreamsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 1 日 23:14 UTC
- 编辑时间：2017 年 12 月 1 日 23:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLaunchWizard_Fullaccess

AmazonLaunchWizard_Fullaccess 是一项 [AWS 托管策略](#)：提供对 AWS Launch 向导和其他必要服务的完全访问权限。

使用此策略

您可以将 AmazonLaunchWizard_Fullaccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 6 日 17:47 UTC
- 编辑时间：2023 年 2 月 22 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLaunchWizardFullAccessV2

AmazonLaunchWizardFullAccessV2 是一项 [AWS 托管策略](#)：提供对 AWS Launch 向导和其他必要服务的完全访问权限。

使用此策略

您可以将 AmazonLaunchWizardFullAccessV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 1 日 17:14 UTC
- 编辑时间：2023 年 9 月 1 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLexChannelsAccess

AmazonLexChannelsAccess 是一项 [AWS 托管策略](#)：此策略允许客户从通道调用 Lex 运行时系统

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 1 月 13 日 20:12 UTC

- 编辑时间：2021 年 1 月 13 日 20:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLexFullAccess

AmazonLexFullAccess 是一项 [AWS 托管策略](#)：通过提供对 Amazon Lex 的完全访问权限 AWS Management Console。此外还提供创建 Lex 服务关联角色的权限，并授予 Lex 调用一组有限的 Lambda 函数的权限。

使用此策略

您可以将 AmazonLexFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:20 UTC
- 编辑时间：世界标准时间 2024 年 2 月 7 日 00:55
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexReadOnly

AmazonLexReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Lex 的只读访问权限。

使用此策略

您可以将 AmazonLexReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:13 UTC
- 编辑时间：2023 年 1 月 31 日 19:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLexReplicationPolicy

AmazonLexReplicationPolicy 是一项 [AWS 托管策略](#)：允许 Amazon Lex 代表您跨区域复制 Lex 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 1 月 31 日 23:29
- 编辑时间：世界标准时间 2024 年 3 月 8 日 17:11
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonLexRunBotsOnly

AmazonLexRunBotsOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Lex 对话 API 的访问权限。

使用此策略

您可以将 AmazonLexRunBotsOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 11 日 23:06 UTC
- 编辑时间：2021 年 8 月 18 日 00:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLexV2BotPolicy

AmazonLexV2BotPolicy 是一项 [AWS 托管策略](#)：为 Lex V2 机器人提供代表您调用其他 AWS 服务的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 1 月 13 日 20:10 UTC
- 编辑时间：2021 年 1 月 13 日 20:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutEquipmentFullAccess

AmazonLookoutEquipmentFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Equipment 操作的完全访问权限

使用此策略

您可以将 AmazonLookoutEquipmentFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 8 日 15:52 UTC
- 编辑时间：2021 年 11 月 24 日 21:00 UTC

- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutEquipmentReadOnlyAccess

AmazonLookoutEquipmentReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Equipment 的只读访问权限

使用此策略

您可以将 AmazonLookoutEquipmentReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 5 日 16:47 UTC
- 编辑时间：2022 年 11 月 10 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutMetricsFullAccess

AmazonLookoutMetricsFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Metrics 的所有操作的访问权限

使用此策略

您可以将 AmazonLookoutMetricsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 5 月 7 日 00:43 UTC
- 编辑时间 : 2021 年 5 月 7 日 00:43 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutMetricsReadOnlyAccess

AmazonLookoutMetricsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Metrics 的所有只读操作的访问权限

使用此策略

您可以将 AmazonLookoutMetricsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 7 日 00:43 UTC
- 编辑时间：2022 年 1 月 4 日 18:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutVisionConsoleFullAccess

AmazonLookoutVisionConsoleFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Vision 的完全访问权限，以及对所需服务和控制台依赖项的限定访问权限。

使用此策略

您可以将 AmazonLookoutVisionConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 5 月 11 日 19:37 UTC
- 编辑时间 : 2021 年 5 月 11 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutVisionConsoleReadOnlyAccess

AmazonLookoutVisionConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Vision 的只读访问权限，以及对所需服务和控制台依赖项的限定访问权限。

使用此策略

您可以将 AmazonLookoutVisionConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 5 月 11 日 19:32 UTC
- 编辑时间 : 2021 年 12 月 9 日 02:46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutVisionFullAccess

AmazonLookoutVisionFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Vision 的完全访问权限，以及对所需依赖项的限定访问权限。

使用此策略

您可以将 AmazonLookoutVisionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 5 月 11 日 19:24 UTC
- 编辑时间 : 2021 年 5 月 11 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonLookoutVisionReadOnlyAccess

AmazonLookoutVisionReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Lookout for Vision 的只读访问权限，以及对所需依赖项的限定访问权限。

使用此策略

您可以将 AmazonLookoutVisionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 11 日 19:11 UTC
- 编辑时间：2021 年 12 月 9 日 03:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningBatchPredictionsAccess

AmazonMachineLearningBatchPredictionsAccess 是一项 [AWS 托管策略](#)：授予用户请求 Amazon Machine Learning 批量预测的权限。

使用此策略

您可以将 AmazonMachineLearningBatchPredictionsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:12 UTC
- 编辑时间：2015 年 4 月 9 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning>DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningCreateOnlyAccess

AmazonMachineLearningCreateOnlyAccess 是一项 [AWS 托管策略](#)：为非预测式 Amazon Machine Learning 资源提供创建权限。

使用此策略

您可以将 AmazonMachineLearningCreateOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 4 月 9 日 17:18 UTC
- 编辑时间：2016 年 6 月 29 日，20:55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning>Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningFullAccess

AmazonMachineLearningFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Machine Learning 资源的完全访问权限。

使用此策略

您可以将 AmazonMachineLearningFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:25 UTC
- 编辑时间：2015 年 4 月 9 日 17:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

AmazonMachineLearningManageRealTimeEndpointOnlyAccess 是一项 [AWS 托管策略](#)：授予用户创建和删除 Amazon Machine Learning 模型的实时端点的权限。

使用此策略

您可以将 AmazonMachineLearningManageRealTimeEndpointOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:32 UTC
- 编辑时间：2015 年 4 月 9 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "machinelearning:CreateRealtimeEndpoint",
    "machinelearning>DeleteRealtimeEndpoint"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningReadOnlyAccess

AmazonMachineLearningReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Machine Learning 资源的只读访问权限。

使用此策略

您可以将 AmazonMachineLearningReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 4 月 9 日 17:40 UTC
- 编辑时间：2015 年 4 月 9 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningRealTimePredictionOnlyAccess

AmazonMachineLearningRealTimePredictionOnlyAccess 是一项 [AWS 托管策略](#)：授予用户请求 Amazon Machine Learning 实时预测的权限。

使用此策略

您可以将 AmazonMachineLearningRealTimePredictionOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 4 月 9 日 17:44 UTC
- 编辑时间：2015 年 4 月 9 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonMachineLearningRealTimePredictionOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMachineLearningRoleforRedshiftDataSourceV3

AmazonMachineLearningRoleforRedshiftDataSourceV3 是一项 [AWS 托管策略](#)：允许 Machine Learning 为 Redshift 数据来源配置和使用您的 Redshift 集群和 S3 暂存位置。

使用此策略

您可以将 AmazonMachineLearningRoleforRedshiftDataSourceV3 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 24 日 18:00 UTC
- 编辑时间：2020 年 6 月 24 日 18:00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMacieFullAccess

AmazonMacieFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Macie 的完全访问权限。

使用此策略

您可以将 AmazonMacieFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 14:54 UTC
- 编辑时间：2022 年 7 月 1 日 00:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMacieHandshakeRole

AmazonMacieHandshakeRole 是一项 [AWS 托管策略](#)：授予创建 Amazon Macie 服务相关角色的权限。

使用此策略

您可以将 AmazonMacieHandshakeRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 6 月 28 日 15:46 UTC
- 编辑时间：2018 年 6 月 28 日 15:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMacieReadOnlyAccess

AmazonMacieReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Macie 的只读访问权限。

使用此策略

您可以将 AmazonMacieReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 15 日 21:50 UTC
- 编辑时间：2023 年 6 月 15 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "macie2:Describe*",
      "macie2:Get*",
      "macie2:List*",
      "macie2:BatchGetCustomDataIdentifiers",
      "macie2:SearchResources"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMacieServiceRole

AmazonMacieServiceRole 是一项 [AWS 托管策略](#)：向 Macie 授予对您账户中的资源依赖项的只读访问权限，以便启用数据分析。

使用此策略

您可以将 AmazonMacieServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 14:53 UTC
- 编辑时间：2017 年 8 月 14 日 14:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMacieServiceRolePolicy

AmazonMacieServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon Macie 的服务相关角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 19 日 22:17 UTC
- 编辑时间：2022 年 5 月 19 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonManagedBlockchainConsoleFullAccess

AmazonManagedBlockchainConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Managed Blockchain 的完全访问权限

使用此策略

您可以将 AmazonManagedBlockchainConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 4 月 29 日 21:23 UTC
- 编辑时间 : 2019 年 4 月 29 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonManagedBlockchainFullAccess

AmazonManagedBlockchainFullAccess 是一项[AWS托管策略](#)：提供对 Amazon Managed Blockchain 的完全访问权限。

使用此策略

您可以将 AmazonManagedBlockchainFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 29 日 21:39 UTC
- 编辑时间：2019 年 4 月 29 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "managedblockchain:*"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonManagedBlockchainReadOnlyAccess

AmazonManagedBlockchainReadOnlyAccess 是一项[AWS托管策略](#)：提供对 Amazon Managed Blockchain 的只读访问权限。

使用此策略

您可以将 AmazonManagedBlockchainReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 30 日 18:17 UTC
- 编辑时间：2019 年 4 月 30 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonManagedBlockchainServiceRolePolicy

AmazonManagedBlockchainServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 Amazon Managed Blockchain 使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 1 月 17 日 19:51 UTC
- 编辑时间：2020 年 1 月 17 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMCSFullAccess

AmazonMCSFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Managed Apache Cassandra Service 的完全访问权限

使用此策略

您可以将 AmazonMCSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 13:45 UTC
- 编辑时间：2020 年 4 月 17 日 19:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMCSReadOnlyAccess

AmazonMCSReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Managed Apache Cassandra Service 的只读访问权限

使用此策略

您可以将 AmazonMCSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 13:46 UTC
- 编辑时间：2020 年 4 月 17 日 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMechanicalTurkFullAccess

AmazonMechanicalTurkFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Mechanical Turk 中所有 API 的完全访问权限。

使用此策略

您可以将 AmazonMechanicalTurkFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 12 月 11 日 19:08 UTC

- 编辑时间：2015 年 12 月 11 日 19:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMechanicalTurkReadOnly

AmazonMechanicalTurkReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Mechanical Turk 中只读 API 的访问权限。

使用此策略

您可以将 AmazonMechanicalTurkReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 12 月 11 日 19:08 UTC
- 编辑时间 : 2019 年 9 月 25 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMemoryDBFullAccess

AmazonMemoryDBFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon MemoryDB 的完全访问权限。

使用此策略

您可以将 AmazonMemoryDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 8 日 19:24 UTC
- 编辑时间：2021 年 10 月 8 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMemoryDBReadOnlyAccess

AmazonMemoryDBReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon MemoryDB 的只读访问权限。

使用此策略

您可以将 AmazonMemoryDBReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 8 日 19:27 UTC
- 编辑时间：2021 年 10 月 8 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMobileAnalyticsFinancialReportAccess

AmazonMobileAnalyticsFinancialReportAccess 是一项 [AWS 托管策略](#)：提供对所有报告（包括所有应用程序资源的财务数据）的只读访问权限。

使用此策略

您可以将 AmazonMobileAnalyticsFinancialReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMobileAnalyticsFullAccess

AmazonMobileAnalyticsFullAccess 是一项 [AWS 托管策略](#)：提供对所有应用程序资源的完全访问权限。

使用此策略

您可以将 AmazonMobileAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMobileAnalyticsNon-financialReportAccess

AmazonMobileAnalyticsNon-financialReportAccess 是一项 [AWS 托管策略](#)：提供所有应用程序资源的非财务报告的只读访问权限。

使用此策略

您可以将 AmazonMobileAnalyticsNon-financialReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMobileAnalyticsWriteOnlyAccess

AmazonMobileAnalyticsWriteOnlyAccess 是一项 [AWS 托管策略](#)：提供输入所有应用程序资源的事件数据的只写访问权限。（推荐用于 SDK 集成）

使用此策略

您可以将 AmazonMobileAnalyticsWriteOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMonitronFullAccess

AmazonMonitronFullAccess 是一项 [AWS 托管策略](#)：提供管理 Amazon Monitron 的完全访问权限

使用此策略

您可以将 AmazonMonitronFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 2 日 22:40 UTC
- 编辑时间：2022 年 6 月 8 日 16:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMonitronFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMQApiFullAccess

AmazonMQApiFullAccess 是一项 [AWS 托管策略](#)：通过我们的 API/SDK 提供对 AmazonMQ 的完全访问权限。

使用此策略

您可以将 AmazonMQApiFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 18 日 20:31 UTC
- 编辑时间：2020 年 11 月 4 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMQApiReadOnlyAccess

AmazonMQApiReadOnlyAccess 是一项 [AWS 托管策略](#)：通过我们的 API/SDK 提供对 AmazonMQ 的只读访问权限。

使用此策略

您可以将 AmazonMQApiReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 12 月 18 日 20:31 UTC
- 编辑时间 : 2018 年 12 月 18 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMQFullAccess

AmazonMQFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AmazonMQ 的完全访问权限。

使用此策略

您可以将 AmazonMQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 15:28 UTC
- 编辑时间：2020 年 11 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMQReadOnlyAccess

AmazonMQReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AmazonMQ 的只读访问权限。

使用此策略

您可以将 AmazonMQReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 28 日 15:30 UTC
- 编辑时间：2017 年 11 月 28 日 19:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "mq:Describe*",
    "mq:List*",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMQServiceRolePolicy

AmazonMQServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Amazon MQ 的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 4 日 16:07 UTC
- 编辑时间：2020 年 11 月 4 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMSKConnectReadOnlyAccess

AmazonMSKConnectReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon MSK Connect 的只读访问权限

使用此策略

您可以将 AmazonMSKConnectReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 20 日 10:18 UTC
- 编辑时间：2021 年 10 月 18 日 09:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMSKFullAccess

AmazonMSKFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon MSK 的完全访问权限，以及对其依赖项的其他必要权限。

使用此策略

您可以将 AmazonMSKFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 1 月 14 日 22:07 UTC
- 编辑时间 : 2023 年 10 月 18 日 11:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMSKReadOnlyAccess

AmazonMSKReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon MSK 的只读访问权限

使用此策略

您可以将 AmazonMSKReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 14 日 22:28 UTC
- 编辑时间：2019 年 1 月 14 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonMWAAServiceRolePolicy

AmazonMWAAServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon Managed Workflows for Apache Airflow 使用的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 24 日 14:13 UTC
- 编辑时间：2022 年 11 月 17 日 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonNimbleStudio-LaunchProfileWorker

AmazonNimbleStudio-LaunchProfileWorker 是一项 [AWS 托管策略](#)：此策略授予 Nimble Studio Launch Profile 工作线程所需资源的访问权限。将此策略附加到由 Nimble Studio Builder 创建的 EC2 实例。

使用此策略

您可以将 AmazonNimbleStudio-LaunchProfileWorker 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 4 月 28 日 04:47 UTC
- 编辑时间 : 2021 年 4 月 28 日 04:47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonNimbleStudio-StudioAdmin

AmazonNimbleStudio-StudioAdmin 是一项 [AWS 托管策略](#)：该策略授予与 Studio 管理员关联的 Amazon Nimble Studio 资源，以及其他服务中的相关 Studio 资源的访问权限。将此策略附加到与您的 Studio 关联的管理员角色。

使用此策略

您可以将 AmazonNimbleStudio-StudioAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 28 日 04:47 UTC
- 编辑时间：2023 年 9 月 22 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonNimbleStudio-StudioUser

AmazonNimbleStudio-StudioUser 是一项 [AWS 托管策略](#)：该策略授予与 Studio 管理用户关联的 Amazon Nimble Studio 资源，以及其他服务中的相关 Studio 资源的访问权限。将此策略附加到与您的 Studio 关联的用户角色。

使用此策略

您可以将 AmazonNimbleStudio-StudioUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 28 日 04:48 UTC
- 编辑时间：2023 年 9 月 22 日 17:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOmicsFullAccess

AmazonOmicsFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Omics 和其他必需 AWS 服务的完全访问权限。此策略允许用户查看和接受 RAM 共享邀请，以访问用户的 AWS 账户以外的资源。

使用此策略

您可以将 AmazonOmicFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 2 月 24 日 00:59 UTC
- 编辑时间 : 2023 年 2 月 24 日 00:59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOmicsReadOnlyAccess

AmazonOmicsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Omics 的只读访问权限

使用此策略

您可以将 AmazonOmicsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 29 日 04:17 UTC
- 编辑时间：2022 年 11 月 29 日 04:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOneEnterpriseFullAccess

AmazonOneEnterpriseFullAccess 是一项 [AWS 托管策略：该策略](#) 授予管理权限，允许访问所有 Amazon One Enterprise 资源和操作。

使用此策略

您可以将 AmazonOneEnterpriseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 04:58
- 编辑时间：世界标准时间 2023 年 11 月 28 日 04:58
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOneEnterpriseInstallerAccess

AmazonOneEnterpriseInstallerAccess 是一项 [AWS 托管策略](#)：此策略授予有限的读取和写入权限，允许安装和激活设备。

使用此策略

您可以将 AmazonOneEnterpriseInstallerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 05:00
- 编辑时间：世界标准时间 2023 年 11 月 28 日 05:00
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOneEnterpriseReadOnlyAccess

AmazonOneEnterpriseReadOnlyAccess 是一项 [AWS 托管策略：该策略](#) 授予对所有 Amazon One Enterprise 资源和操作的只读权限。

使用此策略

您可以将 AmazonOneEnterpriseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 04:59
- 编辑时间：世界标准时间 2023 年 11 月 28 日 04:59
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchDashboardsServiceRolePolicy

AmazonOpenSearchDashboardsServiceRolePolicy是一项[AWS托管策略](#)，它：提供访问亚马逊 OpenSearch 控制面板服务的权限，以访问其他AWS服务，例如 CloudWatch 代表您访问其他服务

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 12 月 22 日 19:38
- 编辑时间：世界标准时间 2023 年 12 月 22 日 19:38
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchIngestionFullAccess

AmazonOpenSearchIngestionFullAccess 是一项 [AWS 托管策略](#)：允许 Amazon OpenSearch Ingestion 代表您访问其他 AWS 服务。

使用此策略

您可以将 AmazonOpenSearchIngestionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 4 月 26 日 18:11 UTC
- 编辑时间 : 2023 年 4 月 26 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchIngestionReadOnlyAccess

AmazonOpenSearchIngestionReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon OpenSearch Ingestion 服务的只读访问权限

使用此策略

您可以将 AmazonOpenSearchIngestionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 26 日 18:09 UTC
- 编辑时间：2023 年 4 月 26 日 18:09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchIngestionServiceRolePolicy

AmazonOpenSearchIngestionServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon OpenSearch Ingestion 服务代表您访问其他 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 18 日 16:49 UTC
- 编辑时间：2022 年 11 月 18 日 16:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchServerlessServiceRolePolicy

AmazonOpenSearchServerlessServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon OpenSearch 无服务器代表您访问其他 AWS 服务，例如 CloudWatch API。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 24 日 19:50 UTC
- 编辑时间：2022 年 11 月 24 日 19:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchServiceCognitoAccess

AmazonOpenSearchServiceCognitoAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Cognito 配置服务的访问权限。

使用此策略

您可以将 AmazonOpenSearchServiceCognitoAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 2 日 06:31 UTC
- 编辑时间：2021 年 12 月 20 日 14:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchServiceFullAccess

AmazonOpenSearchServiceFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon OpenSearch Service 配置服务的完全访问权限。

使用此策略

您可以将 AmazonOpenSearchServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 8 日 05:33 UTC
- 编辑时间：2021 年 9 月 8 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchServiceReadOnlyAccess

AmazonOpenSearchServiceReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon OpenSearch Service 配置服务的只读访问权限。

使用此策略

您可以将 AmazonOpenSearchServiceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 8 日 05:38 UTC

- 编辑时间：2021 年 9 月 8 日 05:38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonOpenSearchServiceRolePolicy

AmazonOpenSearchServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon OpenSearch Service 代表您访问其他 AWS 服务，例如 EC2 网络 API。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 26 日 09:27 UTC
- 编辑时间：2023 年 10 月 23 日 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPersonalizeFullAccess

AmazonPersonalizeFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Amazon Personalize 的完全访问权限。还提供对相关服务（例如 S3、CloudWatch）的部分访问权限。

使用此策略

您可以将 AmazonPersonalizeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 12 月 4 日 22:24 UTC
- 编辑时间：2019 年 5 月 30 日 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPollyFullAccess

AmazonPollyFullAccess 是一项 [AWS 托管策略](#)：授予对 Amazon Polly 服务和资源的完全访问权限。

使用此策略

您可以将 AmazonPollyFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 18:59 UTC
- 编辑时间：2016 年 11 月 30 日 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPollyReadOnlyAccess

AmazonPollyReadOnlyAccess 是一项 [AWS 托管策略](#)：授予对 Amazon Polly 资源的只读访问权限。

使用此策略

您可以将 AmazonPollyReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 30 日 18:59 UTC
- 编辑时间：2018 年 7 月 17 日 16:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "polly:DescribeVoices",
      "polly:GetLexicon",
      "polly:GetSpeechSynthesisTask",
      "polly:ListLexicons",
      "polly:ListSpeechSynthesisTasks",
      "polly:SynthesizeSpeech"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPrometheusConsoleFullAccess

AmazonPrometheusConsoleFullAccess 是一项 [AWS 托管策略](#)：授予对 AWS 控制台中 AWS Managed Prometheus 资源的完全访问权限

使用此策略

您可以将 AmazonPrometheusConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:11 UTC

- 编辑时间：2022 年 10 月 24 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPrometheusFullAccess

AmazonPrometheusFullAccess 是一项 [AWS 托管策略](#)：授予对 AWS Managed Prometheus 资源的完全访问权限

使用此策略

您可以将 AmazonPrometheusFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:10 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 20:16
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/scrapper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scrapper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```



```
    }  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPrometheusQueryAccess

AmazonPrometheusQueryAccess 是一项 [AWS 托管策略](#)：授予对 AWS Managed Prometheus 资源运行查询的权限

使用此策略

您可以将 AmazonPrometheusQueryAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 19 日 01:02 UTC
- 编辑时间：2020 年 12 月 19 日 01:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPrometheusRemoteWriteAccess

AmazonPrometheusRemoteWriteAccess 是一项 [AWS 托管策略](#)：授予对 AWS Managed Prometheus 工作空间的只写访问权限

使用此策略

您可以将 AmazonPrometheusRemoteWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 19 日 01:04 UTC

- 编辑时间：2020 年 12 月 19 日 01:04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonPrometheusScrapingServiceRolePolicy

AmazonPrometheusScrapingServiceRolePolicy 是一项 [AWS 托管策略](#)，它可以：为 Prometheus Collector 提供对亚马逊托管服务管理或使用的 AWS 资源的访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 14:19
- 编辑时间：世界标准时间 2023 年 11 月 26 日 14:19
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScrapersServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scrapers.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScrapers*"
    },
    {
      "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" : [
          "AMPAgentlessScrapper"
        ]
      }
    }
  },
  {
    "Sid" : "TagManagement",
    "Effect" : "Allow",
    "Action" : "ec2:CreateTags",
    "Resource" : "arn:*:ec2:*:*:network-interface/*",
    "Condition" : {
      "StringEquals" : {
        "ec2:CreateAction" : "CreateNetworkInterface"
      },
      "Null" : {
        "aws:RequestTag/AMPAgentlessScrapper" : "false"
      }
    }
  },
  {
    "Sid" : "ENIUpdating",
    "Effect" : "Allow",
    "Action" : [
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute"
    ],
    "Resource" : "*",
    "Condition" : {
      "Null" : {
        "ec2:ResourceTag/AMPAgentlessScrapper" : "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}"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonQFullAccess

AmazonQFullAccess 是一项 [AWS 托管策略](#)，它：提供完全访问权限以实现与 Amazon Q 的互动

使用此策略

您可以将 AmazonQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 28 日 16:00
- 编辑时间：世界标准时间 2023 年 11 月 28 日 16:00
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonQLDBConsoleFullAccess

AmazonQLDBConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon QLDB 的完全访问权限。

使用此策略

您可以将 AmazonQLDBConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 9 月 5 日 18:24 UTC
- 编辑时间 : 2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonQLDBFullAccess

AmazonQLDBFullAccess 是一项 [AWS 托管策略](#)：提供通过服务 API 访问 Amazon QLDB 的完全访问权限。

使用此策略

您可以将 AmazonQLDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 9 月 5 日 18:23 UTC
- 编辑时间：2022 年 11 月 4 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonQLDBReadOnly

AmazonQLDBReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon QLDB 的只读访问权限。

使用此策略

您可以将 AmazonQLDBReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 9 月 5 日 18:19 UTC
- 编辑时间：2021 年 7 月 2 日 02:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSBetaServiceRolePolicy

AmazonRDSBetaServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon RDS 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 2 日 19:41 UTC
- 编辑时间：2022 年 12 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSCustomInstanceProfileRolePolicy

AmazonRDSCustomInstanceProfileRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon RDS Custom 通过 EC2 实例配置文件执行各种自动化操作和数据库管理任务。

使用此策略

您可以将 AmazonRDSCustomInstanceProfileRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 2 月 27 日 17:42
- 编辑时间：世界标准时间 2024 年 2 月 27 日 17:42

- ARN: arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "cwUploadPermission",
  "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"
      }
    }
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRDSCustomPreviewServiceRolePolicy

AmazonRDSCustomPreviewServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon RDS Custom Preview 服务角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 8 日 21:44 UTC
- 编辑时间：2023 年 9 月 20 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSCustomServiceRolePolicy

AmazonRDSCustomServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon RDS Custom 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 8 日 21:39 UTC
- 编辑时间：2023 年 9 月 20 日 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "RequireIbmsV2",
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSDataFullAccess

AmazonRDSDataFullAccess 是一项 [AWS 托管策略](#)：允许使用 RDS 数据 API、用于 RDS 数据库凭证的密钥存储 API 以及数据库控制台查询管理 API 在 AWS 账户中的 Aurora Serverless 集群上执行 SQL 语句的完全访问权限。

使用此策略

您可以将 AmazonRDSDataFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 20 日 21:29 UTC
- 编辑时间：2019 年 11 月 20 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSDataFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSDirectoryServiceAccess

AmazonRDSDirectoryServiceAccess 是一项 [AWS 托管策略](#)：允许 RDS 代表客户访问已加入域的 SQL Server 数据库实例的 Directory Service 托管 AD。

使用此策略

您可以将 AmazonRDSDirectoryServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 26 日 02:02 UTC
- 编辑时间：2019 年 5 月 15 日 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ds:DescribeDirectories",
      "ds:AuthorizeApplication",
      "ds:UnauthorizeApplication",
      "ds:GetAuthorizedApplicationDetails"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSEnhancedMonitoringRole

AmazonRDSEnhancedMonitoringRole 是一项 [AWS 托管策略](#)：提供访问 Cloudwatch 以实现 RDS 增强型监控的权限

使用此策略

您可以将 AmazonRDSEnhancedMonitoringRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 11 日 19:58 UTC
- 编辑时间：2015 年 11 月 11 日 19:58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSFullAccess

AmazonRDSFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon RDS 的完全访问权限。

使用此策略

您可以将 AmazonRDSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 8 月 17 日 23:00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSFullAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSPerformanceInsightsFullAccess

AmazonRDSPerformanceInsightsFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 RDS Performance Insights 的完全访问权限

使用此策略

您可以将 AmazonRDSPerformanceInsightsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 15 日 23:41 UTC
- 编辑时间：2023 年 10 月 23 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSPerformanceInsightsReadOnly

AmazonRDSPerformanceInsightsReadOnly 是一项 [AWS 托管策略](#)：RDS Performance Insights 的只读策略

使用此策略

您可以将 AmazonRDSPerformanceInsightsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 5 日 00:02 UTC
- 编辑时间：2023 年 10 月 23 日 21:17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSPreviewServiceRolePolicy

AmazonRDSPreviewServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon RDS Preview 服务角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 31 日 18:02 UTC
- 编辑时间：2023 年 10 月 4 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSReadOnlyAccess

AmazonRDSReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon RDS 的只读访问权限。

使用此策略

您可以将 AmazonRDSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2023 年 4 月 14 日 12:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRDSServiceRolePolicy

AmazonRDSServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon RDS 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 1 月 8 日 18:17 UTC
- 编辑时间：世界标准时间 2024 年 1 月 19 日 15:10
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy

策略版本

策略版本：v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRedshiftAllCommandsFullAccess

AmazonRedshiftAllCommandsFullAccess 是一项 [AWS 托管策略](#)：此策略包括运行 SQL 命令以复制、加载、卸载、查询和分析 Amazon Redshift 上的数据的权限。此策略还授予权限，以便为相关服务运行 SELECT 语句，例如 Amazon S3、Amazon CloudWatch Logs、Amazon SageMaker 和 AWS Glue。

使用此策略

您可以将 AmazonRedshiftAllCommandsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 4 日 00:48 UTC
- 编辑时间：2021 年 11 月 25 日 02:27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRedshiftDataFullAccess

AmazonRedshiftDataFullAccess 是一项 [AWS 托管策略](#)：此策略提供了对 Amazon Redshift Data API 的完全访问权限。此策略还授予访问其他所需服务的限定访问权限。

使用此策略

您可以将 AmazonRedshiftDataFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 9 日 19:23 UTC
- 编辑时间：2023 年 4 月 7 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
}

```

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRedshiftFullAccess

AmazonRedshiftFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon Redshift 的完全访问权限。

使用此策略

您可以将 AmazonRedshiftFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2022 年 7 月 7 日 23:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```

"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" : "*"
      }
    }
  }
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRedshiftQueryEditor

AmazonRedshiftQueryEditor 是一项 [AWS 托管策略](#)：提供对 Amazon Redshift 查询编辑器和通过 AWS Management Console 保存的查询的完全访问权限。

使用此策略

您可以将 AmazonRedshiftQueryEditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 4 日 22:50 UTC
- 编辑时间：2021 年 2 月 16 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRedshiftQueryEditorV2FullAccess

AmazonRedshiftQueryEditorV2FullAccess 是一项 [AWS 托管策略](#)：授予对 Amazon Redshift 查询编辑器 V2 操作和资源的完全访问权限。此策略还授予访问其他所需服务的访问权限。这包括列出 Amazon Redshift 集群、读取 KMS 中的密钥和别名以及在 AWS Secrets Manager 中管理查询编辑器 V2 密钥的权限。AWS

使用此策略

您可以将 AmazonRedshiftQueryEditorV2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:06 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:20
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2NoSharing

AmazonRedshiftQueryEditorV2NoSharing 是一项 [AWS 托管策略](#)：授予在不共享资源的情况下使用 Amazon Redshift 查询编辑器 V2 的权限。被授予权限的主体只能读取、更新和删除自己的资源，但不能共享这些资源。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2NoSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:18 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:25
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2ReadSharing

AmazonRedshiftQueryEditorV2ReadSharing 是一项 [AWS 托管策略](#)：授予使用 Amazon Redshift 查询编辑器 V2 的权限，并且可以在有限情况下共享资源。获得授权的主体可读取、写入和共享自己的资源。获得授权的主体可读取其与团队共享的资源，但不能更新。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2ReadSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:22 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:27
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:user}"
    }
  }
},
{
  "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}"
    }
  }
}
]
}

```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftQueryEditorV2ReadWriteSharing

AmazonRedshiftQueryEditorV2ReadWriteSharing 是一项 [AWS 托管策略](#)：授予使用 Amazon Redshift 查询编辑器 V2 的权限，并且可以共享资源。获得授权的主体可读取、写入和共享自己的资源。授予主体可以读取和更新与其团队共享的资源。此策略还授予访问其他所需服务的访问权限。这包括在 Secrets Manager 中列出 Amazon Redshift 集群和管理委托人的查询编辑器 V2 密钥的权限。

使用此策略

您可以将 AmazonRedshiftQueryEditorV2ReadWriteSharing 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 24 日 14:25 UTC
- 编辑时间：世界标准时间 2024 年 2 月 21 日 17:30
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:user}"
      }
    }
  },
  {
    "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}"
        }
    }
}
}
]
}

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftReadOnlyAccess

AmazonRedshiftReadOnlyAccess 是一项 [AWS 托管策略](#)：通过提供对 Amazon Redshift 的只读访问权限。AWS Management Console

使用此策略

您可以将 AmazonRedshiftReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2024 年 2 月 8 日 00:24
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRedshiftServiceLinkedRolePolicy

AmazonRedshiftServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Redshift 代表您呼叫 AWS 服务

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 18 日 19:19 UTC
- 编辑时间：世界标准时间 2024 年 3 月 15 日 20:00
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy

策略版本

策略版本 : v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonRekognitionCustomLabelsFullAccess

AmazonRekognitionCustomLabelsFullAccess 是一项 [AWS 托管策略](#)：此策略指定了 Amazon Rekognition Custom Labels 功能所需的识别和 s3 权限。

使用此策略

您可以将 AmazonRekognitionCustomLabelsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 8 日 19:18 UTC

- 编辑时间：2022 年 8 月 16 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRekognitionFullAccess

AmazonRekognitionFullAccess 是一项 [AWS 托管策略](#)：访问所有 Amazon Rekognition API

使用此策略

您可以将 AmazonRekognitionFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2016 年 11 月 30 日 14:40 UTC
- 编辑时间：2016 年 11 月 30 日 14:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRekognitionReadOnlyAccess

AmazonRekognitionReadOnlyAccess 是一项 [AWS 托管策略](#)：访问所有读取 Rekognition API

使用此策略

您可以将 AmazonRekognitionReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 11 月 30 日 14:58 UTC
- 编辑时间 : 2023 年 11 月 8 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess

策略版本

策略版本 : v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRekognitionServiceRole

AmazonRekognitionServiceRole 是一项 [AWS 托管策略](#)：允许 Rekognition 代表您调用 AWS 服务。

使用此策略

您可以将 AmazonRekognitionServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 29 日 16:52 UTC
- 编辑时间：2017 年 11 月 29 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53AutoNamingFullAccess

AmazonRoute53AutoNamingFullAccess 是一项 [AWS 托管策略](#)：提供对所有 Route 53 Auto Naming 操作的完全访问权限。

使用此策略

您可以将 AmazonRoute53AutoNamingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 1 月 18 日 18:40 UTC
- 编辑时间：2018 年 1 月 18 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53AutoNamingReadOnlyAccess

AmazonRoute53AutoNamingReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 Route 53 Auto Naming 操作的只读访问权限。

使用此策略

您可以将 AmazonRoute53AutoNamingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 1 月 18 日 03:02 UTC
- 编辑时间：2018 年 1 月 18 日 03:02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53AutoNamingRegistrantAccess

AmazonRoute53AutoNamingRegistrantAccess 是一项 [AWS 托管策略](#)：提供对 Route 53 Auto Naming 操作的注册者级别访问权限。

使用此策略

您可以将 AmazonRoute53AutoNamingRegistrantAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 12 日 22:33 UTC
- 编辑时间：2018 年 3 月 12 日 22:33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53DomainsFullAccess

AmazonRoute53DomainsFullAccess 是一项 [AWS 托管策略](#)：提供对所有 Route53 Domains 操作的完全访问权限，并提供“创建托管区”以允许在域注册过程中创建“托管区”。

使用此策略

您可以将 AmazonRoute53DomainsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess` 是一项 [AWS 托管策略](#)：提供对 Route53 Domains 列表和操作的访问权限。

使用此策略

您可以将 AmazonRoute53DomainsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53FullAccess

AmazonRoute53FullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有 Amazon Route 53 的完全访问权限。

使用此策略

您可以将 AmazonRoute53FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 12 月 20 日 21:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53ReadOnlyAccess

AmazonRoute53ReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有 Amazon Route 53 的只读访问权限。

使用此策略

您可以将 AmazonRoute53ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2016 年 11 月 15 日 21:15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryClusterFullAccess

AmazonRoute53RecoveryClusterFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery 集群的完全访问权限

使用此策略

您可以将 AmazonRoute53RecoveryClusterFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:37 UTC
- 编辑时间：2021 年 8 月 18 日 18:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryClusterReadOnlyAccess

AmazonRoute53RecoveryClusterReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery 集群的只读访问权限

使用此策略

您可以将 AmazonRoute53RecoveryClusterReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 17:36 UTC
- 编辑时间：2022 年 4 月 1 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "route53-recovery-cluster:GetRoutingControlState",
    "route53-recovery-cluster:ListRoutingControls"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryControlConfigFullAccess

AmazonRoute53RecoveryControlConfigFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery Control Config 的完全访问权限

使用此策略

您可以将 AmazonRoute53RecoveryControlConfigFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 17:48 UTC
- 编辑时间：2021 年 8 月 18 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryControlConfigReadOnlyAccess

AmazonRoute53RecoveryControlConfigReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery Control Config 的只读访问权限

使用此策略

您可以将 AmazonRoute53RecoveryControlConfigReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:01 UTC

- 编辑时间：2023 年 10 月 18 日 17:15 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonRoute53RecoveryControlConfigReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryReadinessFullAccess

AmazonRoute53RecoveryReadinessFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery Readiness 的完全访问权限

使用此策略

您可以将 AmazonRoute53RecoveryReadinessFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 16:45 UTC
- 编辑时间：2021 年 8 月 18 日 16:45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ]
    }
  ]
}
```



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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53RecoveryReadinessReadOnlyAccess

AmazonRoute53RecoveryReadinessReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Route 53 Recovery Readiness 的只读访问权限

使用此策略

您可以将 AmazonRoute53RecoveryReadinessReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 18 日 18:11 UTC
- 编辑时间：2021 年 11 月 9 日 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53ResolverFullAccess

AmazonRoute53ResolverFullAccess 是一项 [AWS 托管策略](#)：Route 53 Resolver 的完全访问策略

使用此策略

您可以将 AmazonRoute53ResolverFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 30 日 18:10 UTC
- 编辑时间：2020 年 7 月 17 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonRoute53ResolverReadOnlyAccess

AmazonRoute53ResolverReadOnlyAccess 是一项 [AWS 托管策略](#)：Route 53 Resolver 的只读策略

使用此策略

您可以将 AmazonRoute53ResolverReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 30 日 18:11 UTC
- 编辑时间：2019 年 9 月 27 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonS3FullAccess

AmazonS3FullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有桶的完全访问权限。

使用此策略

您可以将 AmazonS3FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2021 年 9 月 27 日 20:16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonS3ObjectLambdaExecutionRolePolicy

AmazonS3ObjectLambdaExecutionRolePolicy 是一项 [AWS 托管策略](#)：提供 AWS Lambda 函数与 Amazon S3 对象 Lambda 交互的权限。还授予 Lambda 写入 CloudWatch Logs 的权限。

使用此策略

您可以将 AmazonS3ObjectLambdaExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 8 月 18 日 10:07 UTC
- 编辑时间：2021 年 8 月 18 日 10:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ]
    }
  ],
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonS3OutpostsFullAccess

AmazonS3OutpostsFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon S3 on Outposts 的完全访问权限。

使用此策略

您可以将 AmazonS3OutpostsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 2 日 17:26 UTC
- 编辑时间：2020 年 10 月 2 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonS3OutpostsReadOnlyAccess

AmazonS3OutpostsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon S3 on Outposts 的只读访问权限。

使用此策略

您可以将 AmazonS3OutpostsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 2 日 18:55 UTC
- 编辑时间：2020 年 10 月 2 日 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonS3ReadOnlyAccess

AmazonS3ReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问所有桶的只读访问权限。

使用此策略

您可以将 AmazonS3ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 8 月 10 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",

```

```
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS 服务 Catalog 服务用于预置 Amazon SageMaker 产品组合中的产品的服务角色策略。向一组相关服务授予权限，包括 CodePipeline、CodeBuild、CodeCommit、Glue、CloudFormation 等。

使用此策略

您可以将 AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 27 日 18:48 UTC
- 编辑时间：2022 年 8 月 2 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasAIServicesAccess

AmazonSageMakerCanvasAIServicesAccess 是一项 [AWS 托管策略](#)：为 Amazon SageMaker Canvas 提供使用人工智能服务的权限，以支持即用型人工智能解决方案。随着 Amazon C SageMaker canvas 增加支持，该政策将为服务添加更多变更权限。

使用此策略

您可以将 AmazonSageMakerCanvasAIServicesAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 23 日 22:36 UTC
- 编辑时间：世界标准时间 2023 年 11 月 29 日 14:47
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



```
"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"
    }
  }
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasBedrockAccess

AmazonSageMakerCanvasBedrockAccess 是一项 [AWS 托管策略](#)：该策略通过提供对 S3 等下游服务的访问权限来授予在 C SageMaker anvas 中使用 Amazon Bedrock 的权限。

使用此策略

您可以将 AmazonSageMakerCanvasBedrockAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 2 月 2 日 18:37
- 编辑时间：世界标准时间 2024 年 2 月 2 日 18:37
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasDataPrepFullAccess

AmazonSageMakerCanvasDataPrepFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon SageMaker 资源和操作的完全访问权限，以便在 Canvas 中准备数据。该策略还提供对相关服务（例如 S3、IAM、KMS、RDS、Lambda、CloudWatch、ECS、EKS、Elasticsearch、EMR、Glue、Secrets Manager）的精选访问权限。EventBridge 此政策应附加到 Amazon SageMaker 域名/用户配置文件执行角色。

使用此策略

您可以将 AmazonSageMakerCanvasDataPrepFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 10 月 27 日 22:56 UTC
- 编辑时间：世界标准时间 2023 年 12 月 8 日 02:53
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasDirectDeployAccess

AmazonSageMakerCanvasDirectDeployAccess 是一项 [AWS 托管策略](#)：允许 Amazon SageMaker Canvas 创建、管理和查看通过 Canvas 创建的端点的端点详细信息。允许 Amazon SageMaker Canvas 从 CloudWatch 检索端点调用指标。

使用此策略

您可以将 AmazonSageMakerCanvasDirectDeployAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 10 月 6 日 18:11 UTC
- 编辑时间：2023 年 10 月 6 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasForecastAccess

AmazonSageMakerCanvasForecastAccess 是一项 [AWS 托管策略](#)：该策略授予在 Amazon Forecast 中使用 SageMaker Canvas 通常所需的权限。

使用此策略

您可以将 AmazonSageMakerCanvasForecastAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 8 月 24 日 20:04 UTC
- 编辑时间：2022 年 8 月 24 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCanvasFullAccess

AmazonSageMakerCanvasFullAccess 是一项 [AWS 托管策略](#)，它提供对 Amazon SageMaker Canvas 资源和操作的完全访问权限。该策略还提供对相关服务（例如 S3、IAM、VPC、ECR、Lambda、CloudWatch logs、Redshift、Secrets Manager 和 Forecast）的精选访问权限。此策略应附加到 Amazon SageMaker 域名/用户配置文件执行角色。

使用此策略

您可以将 AmazonSageMakerCanvasFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 9 日 00:44 UTC

- 编辑时间：世界标准时间 2024 年 1 月 24 日 22:01
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
}

```



```
    }  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerClusterInstanceRolePolicy

AmazonSageMakerClusterInstanceRolePolicy 是一项 [AWS 托管策略：该策略](#) 授予使用 Amazon SageMaker 通常所需的权限。

使用此策略

您可以将 AmazonSageMakerClusterInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 15:11
- 编辑时间：世界标准时间 2023 年 11 月 29 日 15:11
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerCoreServiceRolePolicy

AmazonSageMakerCoreServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon SageMaker 核心服务的核心角色托管策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 21 日 21:40 UTC
- 编辑时间：2020 年 12 月 21 日 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerEdgeDeviceFleetPolicy

AmazonSageMakerEdgeDeviceFleetPolicy 是一项 [AWS 托管策略](#)：为 SageMaker Edge 提供使用默认云连接为客户创建和管理设备实例集所需的权限。

使用此策略

您可以将 AmazonSageMakerEdgeDeviceFleetPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 8 日 16:17 UTC
- 编辑时间：2020 年 12 月 8 日 16:17 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerFeatureStoreAccess

AmazonSageMakerFeatureStoreAccess 是一项 [AWS 托管策略](#)：提供为 Amazon SageMaker FeatureStore 特征组启用离线商店所需的权限。

使用此策略

您可以将 AmazonSageMakerFeatureStoreAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 16:24 UTC
- 编辑时间：2022 年 12 月 5 日 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerFullAccess

AmazonSageMakerFullAccess 是一项 [AWS 托管策略](#)：SageMaker 通过 AWS Management Console 和 SDK 提供对 Amazon 的完全访问权限。还提供对相关服务（例如 S3、ECR、CloudWatch 日志）的精选访问权限。

使用此策略

您可以将 AmazonSageMakerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 13:07 UTC
- 编辑时间：世界标准时间 2023 年 11 月 30 日 13:40
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerFullAccess

策略版本

策略版本：v25（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerGeospatialExecutionRole

AmazonSageMakerGeospatialExecutionRole 是一项 [AWS 托管策略](#)：该策略提供使用 SageMaker 地理空间通常所需的服务的访问权限。

使用此策略

您可以将 AmazonSageMakerGeospatialExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 11 月 30 日 10:08 UTC
- 编辑时间：2023 年 5 月 10 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerGeospatialFullAccess

AmazonSageMakerGeospatialFullAccess 是一项 [AWS 托管策略](#)：该策略授予的权限允许通过 AWS Management Console 和 SDK 完全访问 Amazon SageMaker 地理空间。

使用此策略

您可以将 AmazonSageMakerGeospatialFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 11 月 30 日 10:06 UTC
- 编辑时间：2022 年 11 月 30 日 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerGroundTruthExecution

AmazonSageMakerGroundTruthExecution 是一项 [AWS 托管策略](#)：提供对运行 SageMaker GroundTruth 标记作业所需的 AWS 服务的访问权限

使用此策略

您可以将 AmazonSageMakerGroundTruthExecution 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 9 日 19:30 UTC
- 编辑时间：2022 年 4 月 29 日 20:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerMechanicalTurkAccess

AmazonSageMakerMechanicalTurkAccess 是一项 [AWS 托管策略](#)：提供针对任何 Workteam 创建 Amazon Amgenteil AI FlowDefinition 资源所需的访问权限。

使用此策略

您可以将 AmazonSageMakerMechanicalTurkAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 12 月 3 日 16:19 UTC
- 编辑时间 : 2019 年 12 月 3 日 16:19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerModelGovernanceUseAccess

AmazonSageMakerModelGovernanceUseAccess 是一项 [AWS 托管策略](#)：该 AWS 托管策略授予使用所有 Amazon SageMaker Governance 功能所需的权限。该策略还提供对相关服务（例如 S3、KMS）的部分访问权限。

使用此策略

您可以将 AmazonSageMakerModelGovernanceUseAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 30 日 08:58 UTC
- 编辑时间：2023 年 7 月 17 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

```
    "Resource" : [
      "arn:aws:s3::*SageMaker*",
      "arn:aws:s3::*Sagemaker*",
      "arn:aws:s3::*sagemaker*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "s3:ListBucket",
      "s3:ListAllMyBuckets"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerModelRegistryFullAccess

AmazonSageMakerModelRegistryFullAccess 是一项 [AWS 托管策略](#)：这是适用于 Sagemaker 中的模型注册表的新托管策略。此策略是一项独立的策略，可以附加到用户角色以访问 Sagemaker 中与模型注册表相关的功能。

使用此策略

您可以将 AmazonSageMakerModelRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 13 日 05:20 UTC
- 编辑时间：2023 年 4 月 13 日 05:20 UTC

- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
    }  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerNotebooksServiceRolePolicy

AmazonSageMakerNotebooksServiceRolePolicy 是一项 [AWS 托管策略](#)：适用于 Amazon SageMaker 笔记本电脑服务相关角色的托管策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 18 日 20:27 UTC
- 编辑时间：2023 年 3 月 9 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  ]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS APIGateway 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 Lambda 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 1 日 15:06 UTC
- 编辑时间：2023 年 8 月 1 日 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS CloudFormation 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 Lambda、APIGateway 和其他服务在内的相关服务子集授予权限。

使用此策略

您可以将

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 1 日 15:06 UTC
- 编辑时间：2023 年 8 月 1 日 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Lambda 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 Secrets Manager 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将 AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 1 日 15:05 UTC
- 编辑时间：2023 年 8 月 1 日 15:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerPipelinesIntegrations

AmazonSageMakerPipelinesIntegrations 是一项 [AWS 托管策略](#)：此 Amazon 托管策略授予在 SageMaker 模型构建管道中使用回调步骤和 Lambda 步骤通常所需的权限。此策略已添加到设置 SageMaker Studio 时可以创建的 AmazonSageMaker-ExecutionRole 中。也可以附加到任何其他用于创作或执行管道的角色。

使用此策略

您可以将 AmazonSageMakerPipelinesIntegrations 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 7 月 30 日 16:35 UTC
- 编辑时间：2023 年 2 月 17 日 21:28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerReadOnly

AmazonSageMakerReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 Amazon SageMaker 的只读访问权限。

使用此策略

您可以将 AmazonSageMakerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 13:07 UTC
- 编辑时间：2021 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS APIGateway 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 CloudWatch Logs 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 3 月 25 日 04:25 UTC
- 编辑时间：2022 年 3 月 25 日 04:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS CloudFormation 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 SageMaker 和其他服务在内的相关服务子集授予权限。

使用此策略

您可以将

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 3 月 25 日 04:26 UTC
- 编辑时间：2022 年 3 月 25 日 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS CodeBuild 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 CodePipeline、CodeBuild 和其他服务在内的相关服务子集授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2022 年 3 月 25 日 04:27 UTC
- 编辑时间：2022 年 3 月 25 日 04:27 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS CodePipeline 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 CodePipeline、CodeBuild 和其他服务在内的相关服务子集授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:53 UTC
- 编辑时间：2022 年 2 月 22 日 09:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS CloudWatch Events 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 CodePipeline 和其他服务在内的相关服务子集授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:53 UTC
- 编辑时间：2022 年 2 月 22 日 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Firehose 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 Firehose 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:54 UTC
- 编辑时间：2022 年 2 月 22 日 09:54 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Glue 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 Glue、S3 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 2 月 22 日 09:51 UTC
- 编辑时间：2022 年 8 月 26 日 19:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Lambda 在 Amazon SageMaker 产品组合的 AWS ServiceCatalog 预置产品中使用的服务角色策略。向包括 ECR、S3 和其他服务在内的相关服务集合授予权限。

使用此策略

您可以将 AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 4 日 16:34 UTC
- 编辑时间：2022 年 4 月 4 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSecurityLakeAdministrator

AmazonSecurityLakeAdministrator 是一项 [AWS 托管策略](#)：提供对 Amazon Security Lake 以及管理 Security Lake 所需的相关服务的完全访问权限。

使用此策略

您可以将 AmazonSecurityLakeAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 30 日 22:04 UTC
- 编辑时间：世界标准时间 2024 年 2 月 23 日 16:01
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/apidestininations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [

```



```
        "securitylake.amazonaws.com",
        "lakeformation.amazonaws.com",
        "apidestinations.events.amazonaws.com"
    ]
}
},
{
    "Sid" : "AllowRolePolicyActionsforSubscribersandSources",
    "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" : "*"
}
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonSecurityLakeMetastoreManager

AmazonSecurityLakeMetastoreManager 是一项 [AWS 托管策略](#)：亚马逊 SecurityLake 元存储管理器 lambda 的政策，允许访问 cloudwatch、S3、Glue 和 SQS。

使用此策略

您可以将 AmazonSecurityLakeMetastoreManager 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2024 年 1 月 23 日 15:26
- 编辑时间：世界标准时间 2024 年 1 月 23 日 15:26
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSecurityLakePermissionsBoundary

AmazonSecurityLakePermissionsBoundary 是一项 [AWS 托管策略](#)：Amazon Security Lake 为第三方自定义源创建 IAM 角色以向数据湖写入数据，为第三方订阅用户使用来自数据湖的数据创建 IAM 角色，并在创建这些角色时使用此策略来定义其权限边界。

使用此策略

您可以将 AmazonSecurityLakePermissionsBoundary 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 29 日 14:11 UTC
- 编辑时间：2022 年 11 月 29 日 14:11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSESFullAccess

AmazonSESFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SES 的完全访问权限。

使用此策略

您可以将 AmazonSESFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:41 UTC
- 编辑时间 : 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESEFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSESReadOnlyAccess

AmazonSESReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SES 的只读访问权限。

使用此策略

您可以将 AmazonSESReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSNSFullAccess

AmazonSNSFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SNS 的完全访问权限。

使用此策略

您可以将 AmazonSNSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "sns:*"  
    ],  
    "Effect" : "Allow",  
    "Resource" : "*" }  
  ]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSNSReadOnlyAccess

AmazonSNSReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SNS 的只读访问权限。

使用此策略

您可以将 AmazonSNSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSNSRole

AmazonSNSRole 是一项 [AWS 托管策略](#)：Amazon SNS 服务角色的默认策略。

使用此策略

您可以将 AmazonSNSRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSQSFullAccess

AmazonSQSFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SQS 的完全访问权限。

使用此策略

您可以将 AmazonSQSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSQSReadOnlyAccess

AmazonSQSReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon SQS 的只读访问权限。

使用此策略

您可以将 AmazonSQSReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2023 年 6 月 15 日 15:37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",

```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMAutomationApproverAccess

AmazonSSMAutomationApproverAccess 是一项 [AWS 托管策略](#)：提供访问权限以查看自动化执行并将批准决策发送到等待批准的自动化

使用此策略

您可以将 AmazonSSMAutomationApproverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 7 日 23:07 UTC
- 编辑时间：2017 年 8 月 7 日 23:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMAutomationRole

AmazonSSMAutomationRole 是一项 [AWS 托管策略](#)：为 EC2 自动化服务提供执行自动化文档中定义的活动的权限

使用此策略

您可以将 AmazonSSMAutomationRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 5 日 22:09 UTC

- 编辑时间：2017 年 7 月 24 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMDirectoryServiceAccess

AmazonSSMDirectoryServiceAccess 是一项 [AWS 托管策略](#)：此策略允许 SSM Agent 代表客户访问 Directory Service 以加入托管实例的域。

使用此策略

您可以将 AmazonSSMDirectoryServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 3 月 15 日 17:44 UTC
- 编辑时间 : 2019 年 3 月 15 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMFullAccess

AmazonSSMFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon SSM 的完全访问权限。

使用此策略

您可以将 AmazonSSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 29 日 17:39 UTC
- 编辑时间：2019 年 11 月 20 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMMaintenanceWindowRole

AmazonSSMMaintenanceWindowRole 是一项 [AWS 托管策略](#)：用于 EC2 维护时段的服务角色

使用此策略

您可以将 AmazonSSMMaintenanceWindowRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 1 日 15:57 UTC
- 编辑时间：2019 年 7 月 27 日 00:16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
    "resource-groups:ListGroupResources"
  ],
  "Resource" : [
    "*"
  ]
},
{
  "Effect" : "Allow",
  "Action" : [
    "tag:GetResources"
  ],
  "Resource" : [
    "*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSManagedEC2InstanceDefaultPolicy

AmazonSSManagedEC2InstanceDefaultPolicy 是一项 [AWS 托管策略](#)：此策略在 EC2 实例上启用 AWS Systems Manager 功能。

使用此策略

您可以将 AmazonSSManagedEC2InstanceDefaultPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 30 日 20:54 UTC
- 编辑时间：2022 年 8 月 30 日 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSManagedEC2InstanceDefaultPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMManagedInstanceCore

AmazonSSMManagedInstanceCore 是一项 [AWS 托管策略](#)：Amazon EC2 角色启用 AWS Systems Manager 服务核心功能的策略。

使用此策略

您可以将 AmazonSSMManagedInstanceCore 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 3 月 15 日 17:22 UTC
- 编辑时间：2019 年 5 月 23 日 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMPatchAssociation

AmazonSSMPatchAssociation 是一项 [AWS 托管策略](#)：为补丁关联操作提供对子实例的访问权限。

使用此策略

您可以将 AmazonSSMPatchAssociation 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 13 日 16:00 UTC
- 编辑时间：2020 年 5 月 13 日 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMReadOnlyAccess

AmazonSSMReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon SSM 的只读访问权限。

使用此策略

您可以将 AmazonSSMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 29 日 17:44 UTC

- 编辑时间：2015 年 5 月 29 日 17:44 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSSMServiceRolePolicy

AmazonSSMServiceRolePolicy 是一项 [AWS 托管策略](#)：提供对由 Amazon SSM 管理或使用的 AWS 资源的访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 13 日 19:20 UTC
- 编辑时间：2022 年 9 月 14 日 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonSumerianFullAccess

AmazonSumerianFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Sumerian 的完全访问权限。

使用此策略

您可以将 AmazonSumerianFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 4 月 24 日 20:14 UTC
- 编辑时间：2018 年 4 月 24 日 20:14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTextractFullAccess

AmazonTextractFullAccess 是一项 [AWS 托管策略](#)：对所有 Amazon Textract API 的访问权限

使用此策略

您可以将 AmazonTexttractFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 19:07 UTC
- 编辑时间：2018 年 11 月 28 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTexttractFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTextractServiceRole

AmazonTextractServiceRole 是一项 [AWS 托管策略](#)：允许 Textract 代表您调用 AWS 服务。

使用此策略

您可以将 AmazonTextractServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 28 日 19:12 UTC
- 编辑时间：2018 年 11 月 28 日 19:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTimestreamConsoleFullAccess

AmazonTimestreamConsoleFullAccess 是一项 [AWS 托管策略](#)：提供使用 AWS Management Console 管理 Amazon Timestream 的完全访问权限。请注意，此策略还向某些 KMS 操作以及管理您保存的查询的操作授予权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

使用此策略

您可以将 AmazonTimestreamConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：2022 年 2 月 1 日 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTimestreamFullAccess

AmazonTimestreamFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Timestream 的完全访问权限。请注意，此策略还授予某些 KMS 操作访问权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

使用此策略

您可以将 AmazonTimestreamFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 9 月 30 日 21:47 UTC
- 编辑时间 : 2021 年 11 月 26 日 23:42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTimestreamInfluxDBFullAccess

AmazonTimestreamInfluxDBFullAccess 是一项 [AWS 托管策略](#)：提供创建、更新、删除和列出 Amazon Timestream InfluxDB 实例以及创建和列出参数组的完全管理权限。有关所需的其他权限，请参阅文档。

使用此策略

您可以将 AmazonTimestreamInfluxDBFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：世界标准时间 2024 年 3 月 14 日 22:53
- 编辑时间：世界标准时间 2024 年 3 月 14 日 22:53
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamInfluxDBServiceRolePolicy

AmazonTimestreamInfluxDBServiceRolePolicy 是一项 [AWS 托管策略](#)：提供创建、更新、删除和列出 Amazon Timestream InfluxDB 实例以及创建和列出参数组的完全管理权限。有关所需的其他权限，请参阅文档。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 3 月 14 日 18:53
- 编辑时间：世界标准时间 2024 年 3 月 14 日 18:53
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonTimestreamReadOnlyAccess

AmazonTimestreamReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Timestream 的只读访问权限。策略还提供取消任何正在运行的查询的权限。如果使用客户托管的 CMK，请参阅文档了解所需的其他权限。

使用此策略

您可以将 AmazonTimestreamReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 9 月 30 日 21:47 UTC
- 编辑时间 : 2023 年 2 月 28 日 18:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTranscribeFullAccess

AmazonTranscribeFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Transcribe 操作的完全访问权限

使用此策略

您可以将 AmazonTranscribeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 16:06 UTC
- 编辑时间：2018 年 4 月 4 日 16:06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "transcribe:*"
  ],
  "Resource" : "*"
},
{
  "Effect" : "Allow",
  "Action" : [
    "s3:GetObject"
  ],
  "Resource" : [
    "arn:aws:s3::*transcribe*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonTranscribeReadOnlyAccess

AmazonTranscribeReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Transcribe 的只读操作的访问权限

使用此策略

您可以将 AmazonTranscribeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 16:05 UTC

- 编辑时间：2018 年 4 月 4 日 16:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonVPCCrossAccountNetworkInterfaceOperations

AmazonVPCCrossAccountNetworkInterfaceOperations 是一项 [AWS 托管策略](#)：提供创建网络接口并将其附加到跨账户资源的访问权限

使用此策略

您可以将 AmazonVPCCrossAccountNetworkInterfaceOperations 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 7 月 18 日 20:47 UTC
- 编辑时间：2023 年 9 月 25 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCCrossAccountNetworkInterfaceOperations

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonVPCFullAccess

AmazonVPCFullAccess 是一项 [AWS 托管策略](#)：通过提供对 Amazon VPC 的完全访问权限 AWS Management Console。

使用此策略

您可以将 AmazonVPCFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 2 月 8 日 16:03
- ARN: arn:aws:iam::aws:policy/AmazonVPCFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 是一项 [AWS 托管策略](#)：提供描述 AWS 资源、运行网络访问分析器以及在网络洞察访问范围和网络洞察访问范围分析上创建或删除标签的权限。

使用此策略

您可以将 AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 6 月 15 日 22:56 UTC
- 编辑时间 : 2023 年 11 月 3 日 19:31 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonVPCReachabilityAnalyzerFullAccessPolicy

AmazonVPCReachabilityAnalyzerFullAccessPolicy 是一项 [AWS 托管策略](#)：提供描述 AWS 资源、运行 Reachability Analyzer 以及在网络洞察路径和网络洞察分析上创建或删除标签的权限。

使用此策略

您可以将 AmazonVPCReachabilityAnalyzerFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2023 年 6 月 14 日 20:12 UTC
- 编辑时间 : 2023 年 11 月 3 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerFullAccessPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 是一项 [AWS 托管策略](#)：此策略附加到角色 IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess。当管理账户为 Reachability Analyzer 启用可信访问权限时，该角色将部署到组织中的成员账户。该策略提供使用 Reachability Analyzer 控制台查看组织内资源的权限。

使用此策略

您可以将 AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 5 月 1 日 20:38 UTC
- 编辑时间：2023 年 5 月 1 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonVPCReadOnlyAccess

AmazonVPCReadOnlyAccess是一项[AWS 托管策略](#)：通过提供对 Amazon VPC 的只读访问权限 AWS Management Console。

使用此策略

您可以将 AmazonVPCReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：世界标准时间 2024 年 2 月 8 日 17:08

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

策略版本

策略版本 : v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AmazonWorkDocsFullAccess

AmazonWorkDocsFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon WorkDocs 的完全访问权限

使用此策略

您可以将 AmazonWorkDocsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2020 年 4 月 16 日 23:05 UTC
- 编辑时间：2020 年 4 月 16 日 23:05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkDocsReadOnlyAccess

AmazonWorkDocsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon WorkDocs 的只读访问权限

使用此策略

您可以将 AmazonWorkDocsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 1 月 8 日 23:49 UTC
- 编辑时间：2020 年 1 月 8 日 23:49 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkMailEventsServiceRolePolicy

AmazonWorkMailEventsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 Amazon WorkMail Events 使用或管理的 AWS 服务 和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 4 月 16 日 16:52 UTC
- 编辑时间：2019 年 4 月 16 日 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkMailFullAccess

AmazonWorkMailFullAccess 是一项 [AWS 托管策略](#)：提供对 WorkMail、Directory Service、SES、EC2 的完全访问权限以及对 KMS 元数据的读取访问权限。

使用此策略

您可以将 AmazonWorkMailFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 12 月 21 日 14:13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]

```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkMailMessageFlowFullAccess

AmazonWorkMailMessageFlowFullAccess 是一项 [AWS 托管策略](#)：对 WorkMail Message Flow API 的完全访问权限

使用此策略

您可以将 AmazonWorkMailMessageFlowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 11 日 11:08 UTC
- 编辑时间：2021 年 2 月 11 日 11:08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "workmailmessageflow:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkMailMessageFlowReadOnlyAccess

AmazonWorkMailMessageFlowReadOnlyAccess 是一项 [AWS 托管策略](#)：对 GetRawMessageContent API 的 WorkMail 消息的只读访问权限

使用此策略

您可以将 AmazonWorkMailMessageFlowReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 28 日 12:40 UTC
- 编辑时间：2021 年 1 月 28 日 12:40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkMailReadOnlyAccess

AmazonWorkMailReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 WorkMail 和 SES 的只读访问权限。

使用此策略

您可以将 AmazonWorkMailReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2019 年 7 月 25 日 08:24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesAdmin

AmazonWorkSpacesAdmin 是一项 [AWS 托管策略](#)：提供通过 AWS SDK 和 CLI 访问 Amazon WorkSpaces 管理操作的访问权限。

使用此策略

您可以将 AmazonWorkSpacesAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 9 月 22 日 22:21 UTC
- 编辑时间：2023 年 8 月 3 日 23:57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesApplicationManagerAdminAccess

AmazonWorkSpacesApplicationManagerAdminAccess 是一项 [AWS 托管策略](#)：提供在 Amazon WorkSpaces Application Manager 中打包应用程序的管理员访问权限。

使用此策略

您可以将 AmazonWorkSpacesApplicationManagerAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 4 月 9 日 14:03 UTC
- 编辑时间：2015 年 4 月 9 日 14:03 UTC
- ARN: arn:aws:iam::aws:policy/
AmazonWorkspacesApplicationManagerAdminAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkspacesPCAAccess

AmazonWorkspacesPCAAccess 是一项 [AWS 托管策略](#)：此托管策略提供对您的 AWS 账户中的 AWS Certificate Manager Private CA 资源的完全管理访问权限，以进行基于证书的身份验证。

使用此策略

您可以将 AmazonWorkspacesPCAAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 11 月 8 日 00:25 UTC
- 编辑时间 : 2022 年 11 月 8 日 00:25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesSelfServiceAccess

AmazonWorkSpacesSelfServiceAccess 是一项 [AWS 托管策略](#)：提供对 Amazon WorkSpaces 后端服务的访问权限以执行工作区自助服务操作

使用此策略

您可以将 AmazonWorkSpacesSelfServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 19:22 UTC
- 编辑时间：2019 年 6 月 27 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Action" : [
      "workspaces:RebootWorkspaces",
      "workspaces:RebuildWorkspaces",
      "workspaces:ModifyWorkspaceProperties"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesServiceAccess

AmazonWorkSpacesServiceAccess 是一项 [AWS 托管策略](#)：为客户账户提供对 AWS WorkSpaces 服务的访问权限，以启动工作区。

使用此策略

您可以将 AmazonWorkSpacesServiceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 19:19 UTC
- 编辑时间：2020 年 3 月 18 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console、SDK 和 CLI 访问 Amazon WorkSpaces Web 及其依赖项的只读访问权限。

使用此策略

您可以将 AmazonWorkSpacesWebReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 11 月 30 日 14:20 UTC
- 编辑时间：2022 年 11 月 2 日 20:20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonWorkSpacesWebServiceRolePolicy

AmazonWorkSpacesWebServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 Amazon WorkSpaces Web 使用或管理的 AWS 服务 和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 30 日 13:15 UTC
- 编辑时间：2022 年 12 月 15 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonZocaloFullAccess

AmazonZocaloFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Zocalo 的完全访问权限。

使用此策略

您可以将 AmazonZocaloFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmazonZocaloReadOnlyAccess

AmazonZocaloReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Zocalo 的只读访问权限

使用此策略

您可以将 AmazonZocaloReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ]
    }
  ]
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AmplifyBackendDeployFullAccess

AmplifyBackendDeployFullAccess 是一项 [AWS 托管策略](#)：为 Amplify 提供通过 AWS Cloud 开发套件 (CDK) 部署 Amplify 后端资源 (、Amazon AWS AppSync Cognito、Amazon S3 和其他相关服务) 的完全访问权限 AWS

使用此策略

您可以将 AmplifyBackendDeployFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 10 月 6 日 21:32 UTC
- 编辑时间：世界标准时间 2024 年 1 月 2 日 21:13
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
}

```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

APIGatewayServiceRolePolicy

APIGatewayServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 API Gateway 代表客户管理关联的 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 17:23 UTC
- 编辑时间：2021 年 7 月 12 日 22:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AppIntegrationsServiceLinkedRolePolicy

AppIntegrationsServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 AppIntegrations 代表您管理 AppFlow 资源并发布 CloudWatch 指标数据。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 30 日 19:42 UTC
- 编辑时间：2022 年 9 月 30 日 19:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ApplicationAutoScalingForAmazonAppStreamAccess

ApplicationAutoScalingForAmazonAppStreamAccess 是一项 [AWS 托管策略](#)：用于为 Amazon AppStream 启用应用程序自动扩缩的策略

使用此策略

您可以将 ApplicationAutoScalingForAmazonAppStreamAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 2 月 6 日 21:39 UTC
- 编辑时间：2017 年 2 月 6 日 21:39 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 Application Discovery Service 持续导出功能使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 9 日 20:22 UTC
- 编辑时间：2018 年 8 月 13 日 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AppRunnerNetworkingServiceRolePolicy

AppRunnerNetworkingServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS AppRunner Networking 代表您管理相关的 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 1 月 12 日 21:02 UTC
- 编辑时间：2022 年 1 月 12 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AppRunnerServiceRolePolicy

AppRunnerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS AppRunner 代表您管理相关的 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 14 日 19:15 UTC
- 编辑时间：2021 年 5 月 14 日 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingConsoleFullAccess

AutoScalingConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Auto Scaling 的完全访问权限。

使用此策略

您可以将 AutoScalingConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:43 UTC
- 编辑时间：2018 年 2 月 6 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingConsoleReadOnlyAccess

AutoScalingConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Auto Scaling 的只读访问权限。

使用此策略

您可以将 AutoScalingConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:48 UTC
- 编辑时间：2017 年 1 月 12 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingFullAccess

AutoScalingFullAccess 是一项 [AWS 托管策略](#)：提供对 Auto Scaling 的完全访问权限。

使用此策略

您可以将 AutoScalingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:31 UTC
- 编辑时间：2018 年 2 月 6 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingNotificationAccessRole

AutoScalingNotificationAccessRole 是一项 [AWS 托管策略](#)：适用于 AutoScaling Notification Access 服务角色的默认策略。

使用此策略

您可以将 AutoScalingNotificationAccessRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingReadOnlyAccess

AutoScalingReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Auto Scaling 的只读访问权限。

使用此策略

您可以将 AutoScalingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 12 日 19:39 UTC
- 编辑时间：2017 年 1 月 12 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : "autoscaling:Describe*",
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AutoScalingServiceRolePolicy

AutoScalingServiceRolePolicy 是一项 [AWS 托管策略](#)，它：允许访问 Auto Scaling AWS 服务及其使用或管理的资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 1 月 8 日 23:10 UTC
- 编辑时间：世界标准时间 2024 年 2 月 29 日 17:48
- ARN: arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWS_ConfigRole

AWS_ConfigRole 是一个 [AWS 托管策略](#)：AWS Config 服务角色的默认策略。提供 AWS Config 跟踪 AWS 资源更改所需的权限。

使用此策略

您可以将 AWS_ConfigRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 15 日 20:30 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 21:19
- ARN: arn:aws:iam::aws:policy/service-role/AWS_ConfigRole

策略版本

策略版本：v30 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSAccountActivityAccess

AWSAccountActivityAccess 是一项 [AWS 托管策略](#)：允许用户访问“账户活动”页面。

使用此策略

您可以将 AWSAccountActivityAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2023 年 3 月 7 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAccountManagementFullAccess

AWSAccountManagementFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Account Management 的完全访问权限。

使用此策略

您可以将 AWSAccountManagementFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 30 日 23:20 UTC
- 编辑时间：2021 年 9 月 30 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountManagementFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAccountManagementReadOnlyAccess

AWSAccountManagementReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Account Management 的只读访问权限

使用此策略

您可以将 AWSAccountManagementReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 9 月 30 日 23:29 UTC
- 编辑时间：2021 年 9 月 30 日 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAccountUsageReportAccess

AWSAccountUsageReportAccess 是一项 [AWS 托管策略](#)：允许用户访问“账户使用情况报告”页面。

使用此策略

您可以将 AWSAccountUsageReportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAgentlessDiscoveryService

AWSAgentlessDiscoveryService 是一项 [AWS 托管策略](#)：为 Discovery Agentless Connector 提供向 AWS Application Discovery Service 注册的权限。

使用此策略

您可以将 AWSAgentlessDiscoveryService 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 8 月 2 日 01:35 UTC
- 编辑时间：2020 年 2 月 24 日 23:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppFabricFullAccess

AWSAppFabricFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS AppFabric 服务的完全访问权限，以及对其依赖服务（例如 S3、Kinesis、KMS）的只读访问权限。

使用此策略

您可以将 AWSAppFabricFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 19:51 UTC
- 编辑时间：2023 年 6 月 27 日 19:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricFullAccess

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppFabricReadOnlyAccess

AWSAppFabricReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS AppFabric 的只读访问权限

使用此策略

您可以将 AWSAppFabricReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 19:52 UTC
- 编辑时间：2023 年 6 月 27 日 19:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppFabricServiceRolePolicy

AWSAppFabricServiceRolePolicy 是一项 [AWS 托管策略](#)：向 AppFabric 提供代表您访问 AWS 资源的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 26 日 21:07 UTC
- 编辑时间：2023 年 6 月 26 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingAppStreamFleetPolicy

AWSApplicationAutoscalingAppStreamFleetPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 AppStream 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 19:04 UTC
- 编辑时间：2017 年 10 月 20 日 19:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingCassandraTablePolicy

AWSApplicationAutoscalingCassandraTablePolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Cassandra 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 3 月 18 日 22:49 UTC
- 编辑时间：2020 年 3 月 18 日 22:49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingComprehendEndpointPolicy

AWSApplicationAutoscalingComprehendEndpointPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Comprehend 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 14 日 18:39 UTC
- 编辑时间：2019 年 11 月 14 日 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "comprehend:UpdateEndpoint",
      "comprehend:DescribeEndpoint",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoScalingCustomResourcePolicy

AWSApplicationAutoScalingCustomResourcePolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 APIGateway 和 CloudWatch 的权限，以实现自定义资源扩展

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 4 日 23:22 UTC
- 编辑时间：2018 年 6 月 4 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingDynamoDBTablePolicy

AWSApplicationAutoscalingDynamoDBTablePolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 DynamoDB 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 20 日 21:34 UTC
- 编辑时间：2017 年 10 月 20 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 EC2 竞价型实例集和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 25 日 18:23 UTC
- 编辑时间：2017 年 10 月 25 日 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingECSServicePolicy

AWSApplicationAutoscalingECSServicePolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 EC2 Container Service 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 25 日 23:53 UTC
- 编辑时间：2017 年 10 月 25 日 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecs:DescribeServices",
      "ecs:UpdateService",
      "cloudwatch:PutMetricAlarm",
      "cloudwatch:DescribeAlarms",
      "cloudwatch>DeleteAlarms"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingElastiCacheRGPolicy

AWSApplicationAutoscalingElastiCacheRGPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Amazon ElastiCache 和 Amazon CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 17 日 23:41 UTC
- 编辑时间：2021 年 8 月 17 日 23:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingEMRInstanceGroupPolicy

AWSApplicationAutoscalingEMRInstanceGroupPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Elastic Map Reduce 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 26 日 00:57 UTC
- 编辑时间：2017 年 10 月 26 日 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingKafkaClusterPolicy

AWSApplicationAutoscalingKafkaClusterPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Managed Streaming for Apache Kafka 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 24 日 18:36 UTC
- 编辑时间：2020 年 8 月 24 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingLambdaConcurrencyPolicy

AWSApplicationAutoscalingLambdaConcurrencyPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Lambda 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2019 年 10 月 21 日 20:04 UTC
- 编辑时间 : 2019 年 10 月 21 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda>DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch>DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingNeptuneClusterPolicy

AWSApplicationAutoscalingNeptuneClusterPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 Amazon Neptune 和 Amazon CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 2 日 21:14 UTC
- 编辑时间：2021 年 9 月 2 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    ]  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingRDSClusterPolicy

AWSApplicationAutoscalingRDSClusterPolicy 是一项 [AWS 托管策略](#)：该策略向 Application Auto Scaling 授予访问 RDS 和 CloudWatch 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 17 日 17:46 UTC
- 编辑时间：2018 年 8 月 7 日 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationAutoscalingSageMakerEndpointPolicy

AWSApplicationAutoscalingSageMakerEndpointPolicy是一项[AWS托管策略](#)，该策略授予 Application Auto Scaling 访问 SageMaker 和的权限 CloudWatch。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 2 月 6 日 19:58 UTC
- 编辑时间：2023 年 11 月 13 日 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationDiscoveryAgentAccess

AWSApplicationDiscoveryAgentAccess 是一项 [AWS 托管策略](#)：为 Discovery Agent 提供向 AWS Application Discovery Service 注册的权限。

使用此策略

您可以将 AWSApplicationDiscoveryAgentAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 5 月 11 日 21:38 UTC
- 编辑时间：2020 年 2 月 24 日 22:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationDiscoveryAgentlessCollectorAccess

AWSApplicationDiscoveryAgentlessCollectorAccess 是一项 [AWS 托管策略](#)：允许 Application Discovery Service 无代理收集器自动更新、注册 Application Discovery Service 并与之通信

使用此策略

您可以将 `AWSApplicationDiscoveryAgentlessCollectorAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 8 月 16 日 21:00 UTC
- 编辑时间 : 2022 年 8 月 16 日 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationDiscoveryServiceFullAccess

AWSApplicationDiscoveryServiceFullAccess 是一项 [AWS 托管策略](#)：提供查看和标记 AWS Application Discovery Service 维护的配置项目的完全访问权限

使用此策略

您可以将 AWSApplicationDiscoveryServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 5 月 11 日 21:30 UTC
- 编辑时间 : 2019 年 6 月 19 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationAgentInstallationPolicy

AWSApplicationMigrationAgentInstallationPolicy 是一项 [AWS 托管策略](#)：该策略允许安装 AWS Replication Agent，后者与 AWS Application Migration Service (MGN) 配合使用，以将外部服务器迁移到 AWS。将此策略附加到您在 AWS Replication Agent 安装步骤中提供凭证的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationAgentInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 6 月 19 日 07:51 UTC
- 编辑时间：2022 年 9 月 20 日 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationAgentPolicy

AWSApplicationMigrationAgentPolicy 是一项 [AWS 托管策略](#)：该策略允许安装和使用 AWS Replication Agent，后者与 AWS Application Migration Service (MGN) 配合使用，以将外部服务器迁移到 AWS。将此策略附加到您在 AWS Replication Agent 安装步骤中提供凭证的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationAgentPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 4 月 7 日 07:00 UTC
- 编辑时间 : 2022 年 9 月 20 日 11:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationAgentPolicy_v2

AWSApplicationMigrationAgentPolicy_v2 是一项 [AWS 托管策略](#)：该策略允许使用 AWS Replication Agent，后者与 AWS Application Migration Service (MGN) 配合使用，以将外部服务器迁移到 AWS。我们不建议您将此策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationAgentPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 6 月 6 日 14:14 UTC
- 编辑时间：2022 年 6 月 6 日 14:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationConversionServerPolicy

AWSApplicationMigrationConversionServerPolicy 是一项 [AWS 托管策略](#)：该策略允许 Application Migration Service (MGN) 转换服务器 (由 Application Migration Service 启动的 EC2 实例) 与 MGN 服务通信。MGN 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 MGN 转换服务器，由 MGN 在需要时自动启动和终止。我们不建议您将此策略附加到您的 IAM 用户或角色。当用户选择使用 MGN 控制台、CLI 或 API 启动测试或割接实例时，Application Migration Service 会使用 MGN 转换服务器。

使用此策略

您可以将 AWSApplicationMigrationConversionServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 06:48 UTC
- 编辑时间：2021 年 4 月 7 日 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationEC2Access

AWSApplicationMigrationEC2Access 是一项 [AWS 托管策略](#)：此策略提供使用 Application Migration Service (MGN) 将迁移的服务器作为 EC2 实例启动所需的 Amazon EC2 操作。将该策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 07:05 UTC
- 编辑时间：2023 年 2 月 6 日 16:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationFullAccess

AWSApplicationMigrationFullAccess 是一项 [AWS 托管策略](#)：此策略提供 AWS Application Migration Service (MGN) 所有公共 API 的权限，以及读取 KMS 密钥信息的权限。将该策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 06:56 UTC
- 编辑时间：2023 年 4 月 20 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationMGHAccess

AWSApplicationMigrationMGHAccess 是一项 [AWS 托管策略](#)：该策略允许 AWS Application Migration Service (MGN) 将有关使用 MGN 的服务器迁移进度的元数据发送到 AWS Migration Hub (MGH)。MGN 会自动创建附加此策略的 IAM 角色，并使用该角色。我们不建议您将此策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationMGHAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 07:10 UTC
- 编辑时间：2021 年 4 月 7 日 07:10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
```

```
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationReadOnlyAccess

AWSApplicationMigrationReadOnlyAccess 是一项 [AWS 托管策略](#)：该策略为 Application Migration Service (MGN) 的所有只读公有 API 以及其他 AWS 服务的一些只读 API 提供权限，这些 API 是以完全只读的方式使用 MGN 控制台所必需的。将该策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 7 日 07:15 UTC
- 编辑时间：2023 年 3 月 20 日 08:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationReplicationServerPolicy

AWSApplicationMigrationReplicationServerPolicy 是一项 [AWS 托管策略](#)：此策略允许 Application Migration Service (MGN) 复制服务器 (由 Application Migration Service 启动的 EC2 实例) 与 MGN 服务通信，并在您的 AWS 账户 中创建 EBS 快照。Application Migration Service 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 MGN 复制服务器，这些服务器将由 MGN 按需自动启动和终止。作为使用 MGN 管理的迁移过程的一部分，MGN 复制服务器用于促进从外部服务器向 AWS 复制数据。我们不建议您将此策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationReplicationServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 4 月 7 日 07:21 UTC
- 编辑时间：2021 年 4 月 7 日 07:21 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationServiceEc2InstancePolicy

AWSApplicationMigrationServiceEc2InstancePolicy 是一项 [AWS 托管策略](#)：此策略允许安装和使用 AWS Replication Agent，AWS Application Migration Service (AWS MGN) 使用它来迁移在 EC2 (跨区域或跨可用区) 上运行的源服务器。应将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 EC2 实例。

使用此策略

您可以将 AWSApplicationMigrationServiceEc2InstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 22 日 13:19 UTC
- 编辑时间：世界标准时间 2024 年 1 月 3 日 14:19
- ARN: arn:aws:iam::aws:policy/
AWSApplicationMigrationServiceEc2InstancePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationServiceRolePolicy

AWSApplicationMigrationServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Application Migration Service 代表您创建和管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 7 日 06:43 UTC
- 编辑时间：2023 年 6 月 20 日 09:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationSSMAccess

AWSApplicationMigrationSSMAccess 是一项 [AWS 托管策略](#)：该策略提供使用 Application Migration Service (MGN) 执行自定义迁移后命令 SSM 文档所需的 Amazon SSM 操作的访问权限。将该策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 `AWSApplicationMigrationSSMAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 09:29 UTC
- 编辑时间：2023 年 3 月 20 日 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSApplicationMigrationVCenterClientPolicy

AWSApplicationMigrationVCenterClientPolicy 是一项 [AWS 托管策略](#)：该策略允许安装和使用 AWS vCenter Client，后者与 AWS Application Migration Service (MGN) 配合使用，以将外部服务器迁移到 AWS。将此策略附加到您在安装 AWS vCenter Client 时提供其凭证的 IAM 用户或角色。

使用此策略

您可以将 AWSApplicationMigrationVCenterClientPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 8 日 12:53 UTC
- 编辑时间：2021 年 11 月 8 日 12:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshEnvoyAccess

AWSAppMeshEnvoyAccess 是一项 [AWS 托管策略](#)：用于访问虚拟节点配置的 App Mesh Envoy 策略。

使用此策略

您可以将 AWSAppMeshEnvoyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 3 日 21:29 UTC
- 编辑时间：2019 年 7 月 3 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshFullAccess

AWSAppMeshFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS App Mesh API 和管理控制台的完全访问权限。

使用此策略

您可以将 AWSAppMeshFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 16 日 17:50 UTC
- 编辑时间：2021 年 1 月 7 日 19:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshPreviewEnvoyAccess

AWSAppMeshPreviewEnvoyAccess 是一项 [AWS 托管策略](#)：用于访问虚拟节点配置的 App Mesh Preview Envoy 策略。

使用此策略

您可以将 AWSAppMeshPreviewEnvoyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 8 月 5 日 23:32 UTC
- 编辑时间：2019 年 8 月 5 日 23:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshPreviewServiceRolePolicy

AWSAppMeshPreviewServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS App Mesh 使用或管理的 AWS 服务 和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 19 日 19:07 UTC
- 编辑时间：2019 年 8 月 21 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshReadOnly

AWSAppMeshReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS App Mesh API 和管理控制台的只读访问权限。

使用此策略

您可以将 AWSAppMeshReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 4 月 16 日 17:51 UTC
- 编辑时间 : 2021 年 1 月 7 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppMeshServiceRolePolicy

AWSAppMeshServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS AppMesh 使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2019 年 6 月 3 日 18:30 UTC
- 编辑时间：2023 年 10 月 10 日 16:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppRunnerFullAccess

AWSAppRunnerFullAccess 是一项 [AWS 托管策略](#)：授予所有 App Runner 操作的权限。

使用此策略

您可以将 AWSAppRunnerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 1 月 11 日 04:02 UTC
- 编辑时间：2022 年 1 月 11 日 04:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppRunnerReadOnlyAccess

AWSAppRunnerReadOnlyAccess 是一项 [AWS 托管策略](#)：授予列出和查看 App Runner 资源相关详情的权限。

使用此策略

您可以将 AWSAppRunnerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 2 月 24 日 21:24 UTC
- 编辑时间：2022 年 2 月 24 日 21:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppRunnerServicePolicyForECRAccess

AWSAppRunnerServicePolicyForECRAccess 是一项 [AWS 托管策略](#)：这项 AWS App Runner 服务策略授予对客户账户中 Amazon ECR 资源的读取权限。可在创建或更新 App Runner 服务时传递给 App Runner 的角色中使用该策略。

使用此策略

您可以将 AWSAppRunnerServicePolicyForECRAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 5 月 14 日 19:17 UTC
- 编辑时间：2021 年 5 月 14 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppSyncAdministrator

AWSAppSyncAdministrator 是一项 [AWS 托管策略](#)：提供对 AppSync 服务的管理访问权限，但其提供的权限不足以通过控制台进行访问。

使用此策略

您可以将 AWSAppSyncAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:20 UTC
- 编辑时间：2019 年 11 月 4 日 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppSyncInvokeFullAccess

AWSAppSyncInvokeFullAccess 是一项 [AWS 托管策略](#)：提供通过控制台和独立的方式调用 AppSync 服务的完全访问权限

使用此策略

您可以将 AWSAppSyncInvokeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:21 UTC
- 编辑时间：2018 年 3 月 20 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphQLApi",
        "appsync:ListGraphQLApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppSyncPushToCloudWatchLogs

AWSAppSyncPushToCloudWatchLogs 是一项 [AWS 托管策略](#)：允许 AppSync 将日志推送到用户的 CloudWatch 账户。

使用此策略

您可以将 AWSAppSyncPushToCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 4 月 9 日 19:38 UTC
- 编辑时间：2018 年 4 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Effect" : "Allow",
  "Action" : [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppSyncSchemaAuthor

AWSAppSyncSchemaAuthor 是一项 [AWS 托管策略](#)：提供创建、更新和查询 schema 的权限。

使用此策略

您可以将 AWSAppSyncSchemaAuthor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 20 日 21:21 UTC
- 编辑时间：2023 年 2 月 1 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAppSyncServiceRolePolicy

AWSAppSyncServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 AppSync 使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 1 月 21 日 19:56 UTC
- 编辑时间：2020 年 1 月 21 日 19:56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "xray:PutTraceSegments",
      "xray:PutTelemetryRecords",
      "xray:GetSamplingTargets",
      "xray:GetSamplingRules",
      "xray:GetSamplingStatisticSummaries"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSArtifactAccountSync

AWSArtifactAccountSync 是一项 [AWS 托管策略](#)：允许 AWS Artifact 对 AWS Organizations 中的操作进行只读访问。

使用此策略

您可以将 AWSArtifactAccountSync 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 4 月 10 日 23:04 UTC
- 编辑时间：2018 年 4 月 10 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSArtifactReportsReadOnlyAccess

AWSArtifactReportsReadOnlyAccess 是一个 [AWS 托管策略](#)，它：提供对 Artifact 服务 AWS 报告的只读访问权限。

使用此策略

您可以将 AWSArtifactReportsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 1 月 2 日 22:42
- 编辑时间：世界标准时间 2024 年 1 月 2 日 22:42
- ARN: arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSArtifactServiceRolePolicy

AWSArtifactServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Artifact 通过 AWS Organizations 服务收集有关组织的信息。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 8 月 21 日 20:27 UTC
- 编辑时间：2023 年 8 月 21 日 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAuditManagerAdministratorAccess

AWSAuditManagerAdministratorAccess 是一项 [AWS 托管策略](#)：提供管理访问权限，以启用或禁用 AWS Audit Manager、更新设置以及管理评测、控制措施和框架

使用此策略

您可以将 AWSAuditManagerAdministratorAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 11 日 20:02 UTC
- 编辑时间：2022 年 4 月 30 日 00:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAuditManagerServiceRolePolicy

AWSAuditManagerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS Audit Manager 使用或管理的 AWS 服务 和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 8 日 15:12 UTC
- 编辑时间：世界标准时间 2023 年 12 月 6 日 20:39
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSAutoScalingPlansEC2AutoScalingPolicy

AWSAutoScalingPlansEC2AutoScalingPolicy 是一项 [AWS 托管策略](#)：该策略授予 AWS Auto Scaling 权限，以定期预测容量，并为扩展计划中的自动扩缩组生成计划的扩展操作

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 23 日 22:46 UTC
- 编辑时间：2018 年 8 月 23 日 22:46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupAuditAccess

AWSBackupAuditAccess 是一项 [AWS 托管策略](#)：该策略向用户授予创建控制措施和框架的权限，以定义其对 AWS Backup 资源和活动的期望，以及根据其定义的控制措施和框架对 AWS Backup 资源和活动进行审计。此策略向 AWS Config 和类似服务授予描述用户期望和执行审计的权限。此策略还向 S3 和类似服务授予提供审计报告的权限，并使用户能够查找和打开其审计报告。

使用此策略

您可以将 AWSBackupAuditAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 8 月 24 日 01:02 UTC
- 编辑时间：2023 年 4 月 10 日 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupDataTransferAccess

AWSBackupDataTransferAccess 是一项[AWS托管策略](#)：此策略允许 AWS Backint Agent 使用 AWS Backup Storage 平面完成备份数据传输。将此策略附加到使用 Backint Agent 运行 SAP HANA 的 EC2 实例所具有的角色。

使用此策略

您可以将 AWSBackupDataTransferAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 22:48 UTC
- 编辑时间：2022 年 11 月 10 日 22:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupFullAccess

AWSBackupFullAccess 是一项[AWS托管策略](#)：此策略适用于备份管理员，授予对 AWS Backup 操作的完全访问权限，包括创建或编辑备份计划、为备份计划分配AWS资源、删除备份和恢复备份。

使用此策略

您可以将 AWSBackupFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 18 日 22:21 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 27 日 17:33
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

策略版本

策略版本 : v17 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 是一项 [AWS 托管策略](#)：提供代表您同步虚拟机元数据的 AWS BackupGateway 权限

使用此策略

您可以将 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 12 月 15 日 19:43 UTC
- 编辑时间：2022 年 12 月 15 日 19:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupOperatorAccess

AWSBackupOperatorAccess 是一项 [AWS 托管策略](#)：此策略授予用户为备份计划分配 AWS 资源、创建按需备份和恢复备份的权限。此策略不允许用户创建或编辑备份计划，也不允许用户在创建计划备份之后删除这些备份。

使用此策略

您可以将 `AWSBackupOperatorAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 18 日 22:23 UTC
- 编辑时间 : 2023 年 9 月 6 日 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

策略版本

策略版本 : v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupOrganizationAdminAccess

AWSBackupOrganizationAdminAccess 是一项 [AWS 托管策略](#)：此策略适用于使用跨账户备份管理来管理组织备份的备份管理员。

使用此策略

您可以将 AWSBackupOrganizationAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 24 日 16:23 UTC
- 编辑时间：2022 年 11 月 18 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupRestoreAccessForSAPHANA

AWSBackupRestoreAccessForSAPHANA 是一项 [AWS 托管策略](#)：提供在 Amazon EC2 上恢复 SAP HANA 的备份的 AWS Backup 权限

使用此策略

您可以将 AWSBackupRestoreAccessForSAPHANA 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 10 日 22:43 UTC
- 编辑时间：2022 年 11 月 10 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceLinkedRolePolicyForBackup

AWSBackupServiceLinkedRolePolicyForBackup 是一项 [AWS 托管策略](#)：提供代表您跨 AWS 服务创建备份的 AWS Backup 权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 2 日 23:08 UTC
- 编辑时间：世界标准时间 2023 年 12 月 15 日 22:06
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup

策略版本

策略版本：v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceLinkedRolePolicyForBackupTest

AWSBackupServiceLinkedRolePolicyForBackupTest 是一项 [AWS 托管策略](#)：提供代表您跨 AWS 服务创建备份的 AWS Backup 权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 5 月 12 日 17:37 UTC
- 编辑时间：2020 年 5 月 12 日 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceRolePolicyForBackup

AWSBackupServiceRolePolicyForBackup 是一项 [AWS 托管策略](#)：提供代表您跨 AWS 服务创建备份的 AWS Backup 权限

使用此策略

您可以将 AWSBackupServiceRolePolicyForBackup 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 10 日 21:01 UTC
- 编辑时间：世界标准时间 2023 年 12 月 15 日 22:04

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

策略版本

策略版本 : v18 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceRolePolicyForRestores

AWSBackupServiceRolePolicyForRestores 是一项 [AWS 托管策略](#)：提供代表您跨 AWS 服务执行恢复的 AWS Backup 权限。此策略包括创建和删除恢复过程所涉及的 AWS 资源（例如 EBS 卷、RDS 实例和 EFS 文件系统）的权限。

使用此策略

您可以将 AWSBackupServiceRolePolicyForRestores 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 12 日 00:23 UTC
- 编辑时间：世界标准时间 2023 年 12 月 15 日 22:05
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

策略版本

策略版本：v20（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceRolePolicyForS3Backup

AWSBackupServiceRolePolicyForS3Backup 是一项 [AWS 托管策略](#)：该策略包含 AWS Backup 在任何 S3 桶中备份数据所需的权限。其中包括对所有 S3 对象的读取权限以及所有 KMS 密钥的全部解密访问权限。

使用此策略

您可以将 AWSBackupServiceRolePolicyForS3Backup 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 2 月 18 日 17:40 UTC
- 编辑时间 : 2022 年 9 月 1 日 16:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBackupServiceRolePolicyForS3Restore

AWSBackupServiceRolePolicyForS3Restore 是一项 [AWS 托管策略](#)：该策略包含 AWS Backup 将 S3 备份恢复到桶所需的权限。这包括所有 S3 桶的读/写权限，以及所有 KMS 密钥的 GenerateDataKey 和 DescribeKey 权限。

使用此策略

您可以将 AWSBackupServiceRolePolicyForS3Restore 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 2 月 18 日 17:39 UTC
- 编辑时间：2023 年 2 月 7 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBatchFullAccess

AWSBatchFullAccess 是一项 [AWS 托管策略](#)：提供 AWS Batch 资源的完全访问权限。

使用此策略

您可以将 AWSBatchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 6 日 19:35 UTC
- 编辑时间：2022 年 10 月 24 日 16:09 UTC
- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBatchServiceEventTargetRole

AWSBatchServiceEventTargetRole 是一项 [AWS 托管策略](#)：该策略用于为 AWS Batch Job Submission 启用 CloudWatch 事件目标

使用此策略

您可以将 AWSBatchServiceEventTargetRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 2 月 28 日 22:31 UTC
- 编辑时间：2018 年 2 月 28 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBatchServiceRole

AWSBatchServiceRole 是一项 [AWS 托管策略](#)：允许访问相关服务（包括 EC2、Autoscaling、EC2 Container 服务和 Cloudwatch Logs）的 AWS Batch 服务角色策略。

使用此策略

您可以将 AWSBatchServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 6 日 19:36 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 18:49
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole

策略版本

策略版本：v13（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBillingConductorFullAccess

AWSBillingConductorFullAccess 是一项 [AWS 托管策略](#)：使用 AWSBillingConductorFullAccess 托管策略授予对 AWS Billing Conductor (ABC) 控制台和 API 的完全访问权限。此策略允许用户列出、创建和删除 ABC 资源。

使用此策略

您可以将 AWSBillingConductorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 13 日 18:02 UTC
- 编辑时间：2022 年 4 月 13 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBillingConductorReadOnlyAccess

`AWSBillingConductorReadOnlyAccess` 是一项 [AWS 托管策略](#)：使用 `AWSBillingConductorReadOnlyAccess` 托管策略授予对 AWS Billing Conductor (ABC) 控制台和 API 的只读访问权限。此策略授予权限，使其能够查看和列出所有 ABC 资源。它不包括创建或删除资源的能力。

使用此策略

您可以将 `AWSBillingConductorReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 13 日 18:02 UTC
- 编辑时间：2022 年 4 月 13 日 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBillingReadOnlyAccess

AWSBillingReadOnlyAccess 是一项 [AWS 托管策略](#)：允许用户在 Billing Console 中查看账单。

使用此策略

您可以将 AWSBillingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 27 日 20:08 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 18:15
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 是一项 [AWS 托管策略](#)：此策略授予控制 AWS 资源的权限。例如，通过执行 AWS Systems Manager (SSM) 脚本启动和停止 EC2 或 RDS 实例。

使用此策略

您可以将 AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 5 月 25 日 19:03 UTC
- 编辑时间 : 2022 年 5 月 25 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBudgetsActionsWithAWSResourceControlAccess

AWSBudgetsActionsWithAWSResourceControlAccess 是一项 [AWS 托管策略](#)：提供对 AWS 预算操作的完全访问权限，包括使用预算操作通过 AWS Management Console 控制 AWS 资源的运行状态

使用此策略

您可以将 AWSBudgetsActionsWithAWSResourceControlAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 15 日 17:19 UTC
- 编辑时间：2020 年 10 月 15 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/
AWSBudgetsActionsWithAWSResourceControlAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroupsWith",
    "iam:ListPolicies",
    "iam:ListRoles",
    "iam:ListUsers",
    "organizations:ListAccounts",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:ListPolicies",
    "organizations:ListRoots",
    "rds:DescribeDBInstances",
    "sns:ListTopics"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBudgetsReadOnlyAccess

AWSBudgetsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS 预算控制台的只读访问权限。

使用此策略

您可以将 AWSBudgetsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 15 日 17:18 UTC
- 编辑时间：2020 年 10 月 15 日 17:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBugBustFullAccess

AWSBugBustFullAccess 是一项 [AWS 托管策略](#)：此 IAM policy 授予用户对 AWS BugBust 控制台的完全访问权限

使用此策略

您可以将 AWSBugBustFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 6 月 24 日 07:03 UTC
- 编辑时间 : 2021 年 7 月 22 日 20:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBugBustPlayerAccess

AWSBugBustPlayerAccess 是一项 [AWS 托管策略](#)：此 IAM policy 授予用户参与 AWS BugBust 事件的权限

使用此策略

您可以将 AWSBugBustPlayerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 6 月 24 日 07:15 UTC
- 编辑时间：2021 年 6 月 24 日 07:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSBugBustServiceRolePolicy

AWSBugBustServiceRolePolicy 是一项 [AWS 托管策略](#)：向 AWS BugBust 授予代表您访问资源的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 24 日 06:59 UTC
- 编辑时间：2021 年 6 月 24 日 06:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager (ACM) 的完全访问权限

使用此策略

您可以将 AWSCertificateManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 1 月 21 日 17:02 UTC
- 编辑时间 : 2020 年 8 月 17 日 22:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerPrivateCAAuditor

AWSCertificateManagerPrivateCAAuditor 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager 私有证书颁发机构的审计人员访问权限

使用此策略

您可以将 AWSCertificateManagerPrivateCAAuditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:51 UTC
- 编辑时间：2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerPrivateCAFullAccess

AWSCertificateManagerPrivateCAFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager 私有证书颁发机构的完全访问权限

使用此策略

您可以将 AWSCertificateManagerPrivateCAFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:54 UTC
- 编辑时间：2018 年 10 月 23 日 16:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerPrivateCAPrivilegedUser

AWSCertificateManagerPrivateCAPrivilegedUser 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager 私有证书颁发机构的特权证书用户访问权限

使用此策略

您可以将 AWSCertificateManagerPrivateCAPrivilegedUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 20 日 17:43 UTC
- 编辑时间：2019 年 6 月 20 日 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerPrivateCAReadOnly

AWSCertificateManagerPrivateCAReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager 私有证书颁发机构的只读访问权限

使用此策略

您可以将 AWSCertificateManagerPrivateCAReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:57 UTC
- 编辑时间：2020 年 8 月 17 日 22:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerPrivateCAUser

AWSCertificateManagerPrivateCAUser 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager 私有证书颁发机构的证书用户访问权限

使用此策略

您可以将 AWSCertificateManagerPrivateCAUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 23 日 16:53 UTC
- 编辑时间：2019 年 6 月 20 日 17:42 UTC

- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCertificateManagerReadOnly

AWSCertificateManagerReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Certificate Manager (ACM) 的只读访问权限。

使用此策略

您可以将 AWSCertificateManagerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 21 日 17:07 UTC

- 编辑时间：2021 年 3 月 15 日 16:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:GetCertificate",
        "acm:ListTagsForCertificate",
        "acm:GetAccountConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSChatbotServiceLinkedRolePolicy

AWSChatbotServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：AWS Chatbot 使用的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 18 日 16:39 UTC
- 编辑时间：2019 年 11 月 18 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCleanRoomsFullAccess

AWSCleanRoomsFullAccess 是一项 [AWS 托管策略](#)：允许完全访问 AWS 无尘室资源和访问相关资源 AWS 服务。

使用此策略

您可以将 AWSCleanRoomsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:10 UTC
- 编辑时间：世界标准时间 2024 年 3 月 21 日 15:35
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCleanRoomsFullAccessNoQuerying

AWSCleanRoomsFullAccessNoQuerying 是一项 [AWS 托管策略](#)：授予对 AWS Clean Rooms 资源的完全访问权限（但协作中的查询除外）和相关 AWS 服务的访问权限。

使用此策略

您可以将 AWSCleanRoomsFullAccessNoQuerying 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:12 UTC
- 编辑时间：2023 年 7 月 31 日 20:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCleanRoomsMLFullAccess

AWSCleanRoomsMLFullAccess 是一项 [AWS 托管策略](#)：允许完全访问 C AWS lean Rooms 机器学习资源和访问相关资源 AWS 服务。

使用此策略

您可以将 AWSCleanRoomsMLFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 21:02
- 编辑时间：世界标准时间 2023 年 11 月 29 日 21:02
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCleanRoomsMLReadOnlyAccess

AWSCleanRoomsMLReadOnlyAccess 是一项 [AWS 托管策略](#)，它允许 C AWS lean Rooms ML 资源的只读访问权限和对相关的 C AWS lean Rooms 资源的只读访问权限。

使用此策略

您可以将 AWSCleanRoomsMLReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 20:55
- 编辑时间：世界标准时间 2023 年 11 月 29 日 20:55
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCleanRoomsReadOnlyAccess

AWSCleanRoomsReadOnlyAccess 是一项 [AWS 托管策略](#)：允许对 AWS Clean Rooms 资源进行只读访问，以及对相关 AWS Glue 和 Amazon CloudWatch Logs 资源进行只读访问。

使用此策略

您可以将 AWSCleanRoomsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 12 日 16:10 UTC
- 编辑时间：2023 年 1 月 12 日 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloud9Administrator

AWSCloud9Administrator 是一项 [AWS 托管策略](#)：提供对 AWS Cloud9 的管理员访问权限。

使用此策略

您可以将 AWSCloud9Administrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:17 UTC
- 编辑时间：2023 年 10 月 11 日 12:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9Administrator

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloud9EnvironmentMember

AWSCloud9EnvironmentMember 是一项 [AWS 托管策略](#)：提供受邀加入 AWS Cloud9 共享开发环境的能力。

使用此策略

您可以将 AWSCloud9EnvironmentMember 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 30 日 16:18 UTC
- 编辑时间：2023 年 10 月 11 日 12:13 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloud9ServiceRolePolicy

AWSCloud9ServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Cloud9 的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 30 日 13:44 UTC
- 编辑时间：2022 年 1 月 17 日 14:06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloud9SSMInstanceProfile

AWSCloud9SSMInstanceProfile 是一项 [AWS 托管策略](#)：此策略将用于在 InstanceProfile 上附加角色，这将允许 Cloud9 使用 SSM Session Manager 连接到该实例

使用此策略

您可以将 AWSCloud9SSMInstanceProfile 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 14 日 11:40 UTC
- 编辑时间：2020 年 5 月 14 日 11:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloud9User

AWSCloud9User 是一项 [AWS 托管策略](#)：提供创建 AWS Cloud9 开发环境和管理自有环境的权限。

使用此策略

您可以将 AWSCloud9User 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 30 日 16:16 UTC
- 编辑时间 : 2023 年 10 月 11 日 13:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudFormationFullAccess

AWSCloudFormationFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS CloudFormation 的完全访问权限。

使用此策略

您可以将 `AWSCloudFormationFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 26 日 21:50 UTC
- 编辑时间：2019 年 7 月 26 日 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudFormationReadOnlyAccess

AWSCloudFormationReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CloudFormation 的访问权限。

使用此策略

您可以将 AWSCloudFormationReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2019 年 11 月 13 日 17:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudFrontLogger

AWSCloudFrontLogger 是一项 [AWS 托管策略](#)：向 CloudFront Logger 授予对 CloudWatch Logs 的写入权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 6 月 12 日 20:15 UTC
- 编辑时间：2019 年 11 月 22 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudHSMFullAccess

AWSCloudHSMFullAccess 是一项 [AWS 托管策略](#)：提供对所有 CloudHSM 资源的完全访问权限。

使用此策略

您可以将 AWSCloudHSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudHSMReadOnlyAccess

AWSCloudHSMReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 CloudHSM 资源的只读访问权限。

使用此策略

您可以将 AWSCloudHSMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudHSMRole

AWSCloudHSMRole 是一项 [AWS 托管策略](#)：AWS CloudHSM 服务角色的默认策略。

使用此策略

您可以将 AWSCloudHSMRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudMapDiscoverInstanceAccess

AWSCloudMapDiscoverInstanceAccess 是一项 [AWS 托管策略](#)：提供对 AWS Cloud Map 发现 API 的访问权限。

使用此策略

您可以将 AWSCloudMapDiscoverInstanceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 00:02 UTC
- 编辑时间：2023 年 9 月 20 日 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudMapFullAccess

AWSCloudMapFullAccess 是一项 [AWS 托管策略](#)：提供对所有 AWS Cloud Map 操作的完全访问权限。

使用此策略

您可以将 AWSCloudMapFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 23:57 UTC
- 编辑时间：2020 年 7 月 29 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudMapReadOnlyAccess

AWSCloudMapReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 AWS Cloud Map 操作的只读访问权限。

使用此策略

您可以将 AWSCloudMapReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 23:45 UTC
- 编辑时间：2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudMapRegisterInstanceAccess

AWSCloudMapRegisterInstanceAccess 是一项 [AWS 托管策略](#)：提供对 AWS Cloud Map 操作的注册者级别访问权限。

使用此策略

您可以将 AWSCloudMapRegisterInstanceAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 00:04 UTC
- 编辑时间：2023 年 9 月 20 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWS CloudShellFullAccess

AWS CloudShellFullAccess 是一项 [AWS 托管策略](#)：授权使用 AWS CloudShell 的所有功能

使用此策略

您可以将 `AWSCloudShellFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 18:07 UTC
- 编辑时间：2020 年 12 月 15 日 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudTrail_FullAccess

AWSCloudTrail_FullAccess 是一项 [AWS 托管策略](#)：提供对 AWS CloudTrail 的完全访问权限。

使用此策略

您可以将 AWSCloudTrail_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 10 月 8 日 23:41 UTC
- 编辑时间：2021 年 2 月 22 日 19:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  ]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudTrail_ReadOnlyAccess

AWSCloudTrail_ReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS CloudTrail 的只读访问权限。

使用此策略

您可以将 AWSCloudTrail_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 6 月 14 日 17:19 UTC
- 编辑时间：2022 年 6 月 14 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略由名为 AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents 的服务关联角色使用。在 CloudWatch 警报变为 ALARM 状态时，CloudWatch 使用此服务关联角色执行 AWS System Manager Incident Manager 操作。此策略授予代表您启动事件的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 27 日 13:30 UTC
- 编辑时间：2021 年 4 月 27 日 13:30 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeArtifactAdminAccess

AWSCodeArtifactAdminAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeArtifact 的完全访问权限。

使用此策略

您可以将 AWSCodeArtifactAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 6 月 16 日 23:53 UTC
- 编辑时间 : 2020 年 6 月 16 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeArtifactReadOnlyAccess

AWSCodeArtifactReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeArtifact 的只读访问权限。

使用此策略

您可以将 AWSCodeArtifactReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 25 日 21:23 UTC
- 编辑时间：2020 年 6 月 25 日 21:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeBuildAdminAccess

AWSCodeBuildAdminAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeBuild 的完全访问权限。另请附加 `Amazons3ReadOnlyAccess`，以提供下载构建构件的权限，并附加 `IAMFullAccess` 以便为 CodeBuild 创建和管理服务角色。

使用此策略

您可以将 `AWSCodeBuildAdminAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 12 月 1 日 19:04 UTC
- 编辑时间 : 2023 年 7 月 31 日 23:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

策略版本

策略版本 : v13 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeBuildDeveloperAccess

AWSCodeBuildDeveloperAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeBuild 的权限，但不允许执行 CodeBuild 项目管理。另请附加 Amazon3ReadOnlyAccess 以提供下载构建构件的权限。

使用此策略

您可以将 `AWSCodeBuildDeveloperAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 12 月 1 日 19:02 UTC
- 编辑时间 : 2023 年 7 月 31 日 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

策略版本

策略版本 : v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeBuildReadOnlyAccess

AWSCodeBuildReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeBuild 的只读访问权限。另请附加 Amazons3ReadOnlyAccess 以提供下载构建构件的权限。

使用此策略

您可以将 AWSCodeBuildReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 19:03 UTC
- 编辑时间：2020 年 9 月 14 日 16:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeCommitFullAccess

AWSCodeCommitFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeCommit 的完全访问权限。

使用此策略

您可以将 AWSCodeCommitFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:02 UTC
- 编辑时间：2023 年 7 月 17 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitFullAccess

策略版本

策略版本：v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeCommitPowerUser

AWSCodeCommitPowerUser 是一项 [AWS 托管策略](#)：提供对 AWS CodeCommit 存储库的完全访问权限，但不允许删除存储库。

使用此策略

您可以将 AWSCodeCommitPowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 7 月 9 日 17:06 UTC
- 编辑时间 : 2023 年 7 月 17 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

策略版本

策略版本 : v15 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
```



```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeCommitReadOnly

AWSCodeCommitReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeCommit 的只读访问权限。

使用此策略

您可以将 AWSCodeCommitReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:05 UTC
- 编辑时间：2021 年 8 月 18 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitReadOnly

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployDeployerAccess

AWSCodeDeployDeployerAccess 是一项 [AWS 托管策略](#)：提供注册和部署修订版所需的访问权限。

使用此策略

您可以将 AWSCodeDeployDeployerAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 19 日 18:18 UTC

- 编辑时间：2020 年 4 月 2 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployFullAccess

AWSCodeDeployFullAccess 是一项 [AWS 托管策略](#)：提供对 CodeDeploy 资源的完全访问权限。

使用此策略

您可以将 `AWSCodeDeployFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 5 月 19 日 18:13 UTC
- 编辑时间 : 2020 年 4 月 2 日 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployReadOnlyAccess

AWSCodeDeployReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 CodeDeploy 资源的只读访问权限。

使用此策略

您可以将 AWSCodeDeployReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 5 月 19 日 18:21 UTC
- 编辑时间：2020 年 4 月 2 日 16:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRole

AWSCodeDeployRole 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务访问权限，以扩展标签并代表您与 Auto Scaling 交互。

使用此策略

您可以将 AWSCodeDeployRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 5 月 4 日 18:05 UTC
- 编辑时间：2023 年 8 月 16 日 20:38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRoleForCloudFormation

AWSCodeDeployRoleForCloudFormation 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务访问权限，从而代表您调用 Lambda 函数，以通过 CloudFormation 执行蓝绿部署。

使用此策略

您可以将 AWSCodeDeployRoleForCloudFormation 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 5 月 19 日 17:12 UTC
- 编辑时间：2020 年 5 月 19 日 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*
```

```
    "Effect" : "Allow"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRoleForECS

AWSCodeDeployRoleForECS 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务级访问权限，以代表您执行 ECS 蓝绿部署。授予对支持服务的完全访问权限，例如读取所有 S3 对象、调用所有 Lambda 函数、发布到账户内的所有 SNS 主题以及更新所有 ECS 服务的完全访问权限。

使用此策略

您可以将 AWSCodeDeployRoleForECS 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 20:40 UTC
- 编辑时间：2019 年 9 月 23 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRoleForECSLimited

AWSCodeDeployRoleForECSLimited 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务受限访问权限，以代表您执行 ECS 蓝绿部署。

使用此策略

您可以将 AWSCodeDeployRoleForECSLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 20:42 UTC
- 编辑时间：2019 年 9 月 23 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRoleForLambda

AWSCodeDeployRoleForLambda 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务访问权限，以代表您执行 Lambda 部署。

使用此策略

您可以将 AWSCodeDeployRoleForLambda 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 28 日 14:05 UTC
- 编辑时间：2019 年 12 月 3 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeDeployRoleForLambdaLimited

AWSCodeDeployRoleForLambdaLimited 是一项 [AWS 托管策略](#)：提供 CodeDeploy 服务受限访问权限，以代表您执行 Lambda 部署。

使用此策略

您可以将 AWSCodeDeployRoleForLambdaLimited 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2020 年 8 月 17 日 17:14 UTC
- 编辑时间：2020 年 8 月 17 日 17:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodePipeline_FullAccess

AWSCodePipeline_FullAccess是一项[AWS 托管策略](#)，它：AWS CodePipeline 通过提供对的所有访问权限 AWS Management Console。

使用此策略

您可以将 AWSCodePipeline_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 3 日 22:38 UTC
- 编辑时间：世界标准时间 2024 年 3 月 14 日 17:06
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSCodePipeline_ReadOnlyAccess

AWSCodePipeline_ReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodePipeline 的只读访问权限。

使用此策略

您可以将 AWSCodePipeline_ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 3 日 22:25 UTC
- 编辑时间：2020 年 8 月 3 日 22:25 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodePipelineApproverAccess

AWSCodePipelineApproverAccess 是一项 [AWS 托管策略](#)：提供查看和批准所有管道的手动更改的权限

使用此策略

您可以将 AWSCodePipelineApproverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 7 月 28 日 18:59 UTC
- 编辑时间：2017 年 8 月 2 日 17:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodePipelineCustomActionAccess

AWSCodePipelineCustomActionAccess 是一项 [AWS 托管策略](#)：为自定义操作提供访问权限，以轮询作业详细信息（包括临时凭证），并向 AWS CodePipeline 报告状态更新。

使用此策略

您可以将 AWSCodePipelineCustomActionAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:02 UTC
- 编辑时间：2015 年 7 月 9 日 17:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Statement" : [
  {
    "Action" : [
      "codepipeline:AcknowledgeJob",
      "codepipeline:GetJobDetails",
      "codepipeline:PollForJobs",
      "codepipeline:PutJobFailureResult",
      "codepipeline:PutJobSuccessResult"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
],
"Version" : "2012-10-17"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeStarFullAccess

AWSCodeStarFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS CodeStar 的完全访问权限。

使用此策略

您可以将 AWSCodeStarFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 4 月 19 日 16:23 UTC
- 编辑时间：2023 年 3 月 28 日 00:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeStarNotificationsServiceRolePolicy

AWSCodeStarNotificationsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS CodeStar 通知代表您访问 Amazon CloudWatch Events

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 5 日 16:10 UTC
- 编辑时间：2020 年 3 月 19 日 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCodeStarServiceRole

AWSCodeStarServiceRole 是一项 [AWS 托管策略](#)：请勿使用 – AWS CodeStar 服务角色策略，此策略授予管理权限，以便 CodeStar 代表客户管理 IAM 和其他服务资源。

使用此策略

您可以将 AWSCodeStarServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 4 月 19 日 15:20 UTC
- 编辑时间：2021 年 9 月 20 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCompromisedKeyQuarantine

AWSCompromisedKeyQuarantine 是一项 [AWS 托管策略](#)：拒绝访问某些操作，由 AWS 团队在 IAM 用户的凭证遭泄露或公开暴露时应用。请勿删除此策略。相反，您应该会收到有关此事件的电子邮件，请按照其中指定的说明进行操作。

使用此策略

您可以将 AWSCompromisedKeyQuarantine 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 8 月 11 日 18:04 UTC
- 编辑时间 : 2020 年 8 月 11 日 18:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCompromisedKeyQuarantineV2

AWSCompromisedKeyQuarantineV2 是一项 [AWS 托管策略](#)：拒绝访问某些操作，由 AWS 团队在 IAM 用户的凭证遭泄露或公开暴露时应用。请勿删除此策略。相反，请按照为您创建的此事件相关支持案例中指定的说明进行操作。

使用此策略

您可以将 AWSCompromisedKeyQuarantineV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 4 月 21 日 22:30 UTC
- 编辑时间：2023 年 3 月 16 日 00:20 UTC

- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConfigMultiAccountSetupPolicy

AWSConfigMultiAccountSetupPolicy 是一项 [AWS 托管策略](#)：允许 Config 在整个组织中调用 AWS 服务及部署配置资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 17 日 18:03 UTC
- 编辑时间：2023 年 2 月 24 日 01:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConfigRemediationServiceRolePolicy

AWSConfigRemediationServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Config 代表您修复不合规的资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 18 日 21:21 UTC
- 编辑时间：2019 年 6 月 18 日 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConfigRoleForOrganizations

AWSConfigRoleForOrganizations 是一项 [AWS 托管策略](#)：允许 AWS Config 调用只读的 AWS Organizations API

使用此策略

您可以将 AWSConfigRoleForOrganizations 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 3 月 19 日 22:53 UTC
- 编辑时间：2020 年 11 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConfigRulesExecutionRole

AWSConfigRulesExecutionRole 是一项 [AWS 托管策略](#)：允许 AWS Lambda 函数访问 AWS Config API 以及 AWS Config 定期向 Amazon S3 交付的配置快照。对自定义 Config 规则的配置更改执行评估的函数需要此访问权限。

使用此策略

您可以将 AWSConfigRulesExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 3 月 25 日 17:59 UTC
- 编辑时间：2019 年 5 月 13 日 21:33 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConfigServiceRolePolicy

AWSConfigServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Config 代表您调用 AWS 服务并收集资源配置。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 5 月 30 日 23:31 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 17:20
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

策略版本

策略版本：v50 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSConfigUserAccess

AWSConfigUserAccess 是一项 [AWS 托管策略](#)：提供使用 AWS Config 的权限，包括按资源上的标签执行搜索，以及读取所有标签。不提供配置 AWS Config 的权限（这需要管理权限）。

使用此策略

您可以将 AWSConfigUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 18 日 19:38 UTC
- 编辑时间：2019 年 3 月 18 日 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

策略版本

策略版本：v4（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSConnector

AWSConnector 是一项 [AWS 托管策略](#)：允许对所有 EC2 对象进行广泛的读/写访问权限，对以 'import-to-ec2-' 开头的 S3 存储桶进行读/写访问以及列出所有 S3 存储桶的功能，以便 AWS 连接器代表您导入虚拟机。

使用此策略

您可以将 AWSConnector 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 11 日 17:14 UTC
- 编辑时间：2015 年 9 月 28 日 19:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSControlTowerAccountServiceRolePolicy

AWSControlTowerAccountServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Control Tower 代表您调用提供自动账户配置和集中治理的 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 5 日 22:04 UTC
- 编辑时间：2023 年 6 月 5 日 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSControlTowerServiceRolePolicy

AWSControlTowerServiceRolePolicy 是一项 [AWS 托管策略](#)：提供对由 AWS Control Tower 管理或使用的 AWS 资源的访问权限

使用此策略

您可以将 AWSControlTowerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间 : 2019 年 5 月 3 日 18:19 UTC
- 编辑时间 : 2023 年 4 月 12 日 19:15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy

策略版本

策略版本 : v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSCostAndUsageReportAutomationPolicy

AWSCostAndUsageReportAutomationPolicy 是一项 [AWS 托管策略](#)：授予的权限包括描述账户的组织、为 MAP 程序创建 S3 桶并为其应用标签、创建成本和使用情况报告，以及描述成本和使用情况报告定义。

使用此策略

您可以将 AWSCostAndUsageReportAutomationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 1 日 21:27 UTC
- 编辑时间：2021 年 11 月 1 日 21:27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataExchangeFullAccess

AWSDataExchangeFullAccess 是一项 [AWS 托管策略](#)：授予使用 AWS Management Console 和 SDK 对 AWS Data Exchange 及 AWS Marketplace 操作的完全访问权限。它还提供充分利用 AWS Data Exchange 所需的相关服务的部分访问权限。

使用此策略

您可以将 `AWSDataExchangeFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 13 日 19:27 UTC
- 编辑时间 : 2021 年 12 月 2 日 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataExchangeProviderFullAccess

AWSDataExchangeProviderFullAccess 是一项 [AWS 托管策略](#)：授予使用 AWS Management Console 和 SDK 对 AWS Data Exchange 及 AWS Marketplace 操作的数据提供者访问权限。它还提供充分利用 AWS Data Exchange 所需的相关服务的部分访问权限。

使用此策略

您可以将 AWSDataExchangeProviderFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 13 日 19:27 UTC
- 编辑时间 : 2022 年 3 月 15 日 16:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess

策略版本

策略版本 : v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataExchangeReadOnly

AWSDataExchangeReadOnly 是一项 [AWS 托管策略](#)：授予使用 AWS Management Console 和 SDK 对 AWS Data Exchange 及 AWS Marketplace 操作的只读访问权限。

使用此策略

您可以将 AWSDataExchangeReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 13 日 19:27 UTC
- 编辑时间：2021 年 5 月 10 日 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataExchangeSubscriberFullAccess

AWSDataExchangeSubscriberFullAccess 是一项 [AWS 托管策略](#)：授予使用 AWS Management Console 和 SDK 对 AWS Data Exchange 及 AWS Marketplace 操作的数据订阅用户访问权限。它还提供充分利用 AWS Data Exchange 所需的相关服务的部分访问权限。

使用此策略

您可以将 AWSDataExchangeSubscriberFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 13 日 19:27 UTC
- 编辑时间 : 2021 年 11 月 29 日 23:00 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataLifecycleManagerServiceRole

AWSDataLifecycleManagerServiceRole 是一项 [AWS 托管策略](#)：为 AWS Data Lifecycle Manager 提供对 AWS 资源执行操作的相应权限

使用此策略

您可以将 AWSDataLifecycleManagerServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 7 月 6 日 19:34 UTC
- 编辑时间：2022 年 9 月 19 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataLifecycleManagerServiceRoleForAMIManagement

AWSDataLifecycleManagerServiceRoleForAMIManagement 是一项 [AWS 托管策略](#)：为 AWS Data Lifecycle Manager 提供对 AMI 管理的 AWS 资源执行操作的相应权限

使用此策略

您可以将 AWSDataLifecycleManagerServiceRoleForAMIManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 10 月 21 日 19:39 UTC
- 编辑时间：2021 年 8 月 19 日 17:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataLifecycleManagerSSMFullAccess

AWSDataLifecycleManagerSSMFullAccess 是一项 [AWS 托管策略](#)：为 Amazon Data Lifecycle Manager 提供权限，允许其执行在所有 Amazon EC2 实例上运行前置和后置脚本所需的 Systems Manager 操作。

使用此策略

您可以将 AWSDataLifecycleManagerSSMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 10 月 31 日 20:29 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 22:31

- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataPipeline_FullAccess

AWSDataPipeline_FullAccess 是一项 [AWS 托管策略](#)：提供对 Data Pipeline 的完全访问权限，为 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色提供列表访问权限，并为默认角色提供 passRole 访问权限。

使用此策略

您可以将 `AWSDataPipeline_FullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 1 月 19 日 23:14 UTC
- 编辑时间 : 2017 年 8 月 17 日 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataPipeline_PowerUser

AWSDataPipeline_PowerUser 是一项 [AWS 托管策略](#)：提供对 Data Pipeline 的完全访问权限，为 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色提供列表访问权限，并为默认角色提供 passRole 访问权限。

使用此策略

您可以将 AWSDataPipeline_PowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 19 日 23:16 UTC
- 编辑时间：2017 年 8 月 17 日 18:49 UTC

- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataSyncDiscoveryServiceRolePolicy

AWSDataSyncDiscoveryServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 DataSync Discovery 代表您集成其他 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 20 日 22:19 UTC
- 编辑时间：2023 年 3 月 20 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDataSyncFullAccess

AWSDataSyncFullAccess 是一项 [AWS 托管策略](#)，它：提供对其依赖项的完全访问权限 AWS DataSync 和最低限度访问权限

使用此策略

您可以将 AWSDataSyncFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 19:40 UTC
- 编辑时间：世界标准时间 2024 年 2 月 16 日 17:19
- ARN: arn:aws:iam::aws:policy/AWSDataSyncFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSDataSyncReadOnlyAccess

AWSDataSyncReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS DataSync 的只读访问权限

使用此策略

您可以将 AWSDataSyncReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 18 日 19:18 UTC
- 编辑时间：2020 年 6 月 30 日 17:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepLensLambdaFunctionAccessPolicy

AWSDeepLensLambdaFunctionAccessPolicy 是一项 [AWS 托管策略](#)：此策略指定在 DeepLens 设备上运行的 DeepLens 管理 Lambda 函数所需的权限

使用此策略

您可以将 AWSDeepLensLambdaFunctionAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 15:47 UTC
- 编辑时间：2019 年 6 月 11 日 23:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepLensServiceRolePolicy

AWSDeepLensServiceRolePolicy 是一项 [AWS 托管策略](#)：授予 AWS DeepLens 对 AWS 服务以及 DeepLens 及其依赖项（包括物联网、S3、GreenGrass 和 AWS Lambda）所需资源和角色的访问权限。

使用此策略

您可以将 AWSDeepLensServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 29 日 15:46 UTC

- 编辑时间 : 2019 年 9 月 25 日 19:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerAccountAdminAccess

AWSDeepRacerAccountAdminAccess 是一项 [AWS 托管策略](#)：授予 DeepRacer 管理员访问权限，以访问所有操作，包括在多用户模式与单用户模式之间切换。

使用此策略

您可以将 AWSDeepRacerAccountAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 28 日 01:27 UTC
- 编辑时间：2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerCloudFormationAccessPolicy

AWSDeepRacerCloudFormationAccessPolicy 是一项 [AWS 托管策略](#)：允许 CloudFormation 代表您创建和管理 AWS 堆栈和资源。

使用此策略

您可以将 `AWSDeepRacerCloudFormationAccessPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 2 月 28 日 21:59 UTC
- 编辑时间 : 2019 年 6 月 14 日 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerDefaultMultiUserAccess

AWSDeepRacerDefaultMultiUserAccess 是一项 [AWS 托管策略](#)：授予 DeepRacer MultiUser Default 用户访问权限，以在多用户模式下使用 DeepRacer

使用此策略

您可以将 AWSDeepRacerDefaultMultiUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 28 日 01:27 UTC
- 编辑时间：2021 年 10 月 28 日 01:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerFullAccess

AWSDeepRacerFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS DeepRacer 的完全访问权限。还提供对相关服务（例如 S3）的部分访问权限。

使用此策略

您可以将 AWSDeepRacerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 10 月 5 日 22:03 UTC
- 编辑时间 : 2020 年 10 月 5 日 22:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerRoboMakerAccessPolicy

AWSDeepRacerRoboMakerAccessPolicy 是一项 [AWS 托管策略](#)：允许 RoboMaker 代表您创建所需资源并调用 AWS 服务。

使用此策略

您可以将 AWSDeepRacerRoboMakerAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 2 月 28 日 21:59 UTC
- 编辑时间：2019 年 2 月 28 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeepRacerServiceRolePolicy

AWSDeepRacerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 DeepRacer 代表您创建所需资源并调用 AWS 服务。

使用此策略

您可以将 AWSDeepRacerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 2 月 28 日 21:58 UTC
- 编辑时间：2019 年 6 月 12 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDenyAll

AWSDenyAll 是一项 [AWS 托管策略](#)：拒绝所有访问。

使用此策略

您可以将 AWSDenyAll 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 1 日 22:36 UTC
- 编辑时间：世界标准时间 2023 年 12 月 18 日 16:42
- ARN: arn:aws:iam::aws:policy/AWSDenyAll

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeviceFarmFullAccess

AWSDeviceFarmFullAccess 是一项 [AWS 托管策略](#)：提供对所有 AWS Device Farm 操作的完全访问权限。

使用此策略

您可以将 AWSDeviceFarmFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 13 日 16:37 UTC
- 编辑时间：2015 年 7 月 13 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeviceFarmServiceRolePolicy

AWSDeviceFarmServiceRolePolicy 是一项 [AWS 托管策略](#)：向 AWS Device Farm 授予代表您调用 EC2 网络 API 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 20 日 21:02 UTC
- 编辑时间：2022 年 9 月 20 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDeviceFarmTestGridServiceRolePolicy

AWSDeviceFarmTestGridServiceRolePolicy 是一项 [AWS 托管策略](#)：向 AWS Device Farm 授予代表您调用 EC2 API 的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 26 日 22:01 UTC
- 编辑时间：2021 年 5 月 26 日 22:01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDirectConnectFullAccess

AWSDirectConnectFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Direct Connect 的完全访问权限。

使用此策略

您可以将 AWSDirectConnectFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 4 月 30 日 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "directconnect:*",
    "ec2:DescribeVpnGateways",
    "ec2:DescribeTransitGateways"
  ],
  "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDirectConnectReadOnlyAccess

AWSDirectConnectReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Direct Connect 的只读访问权限。

使用此策略

您可以将 AWSDirectConnectReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2020 年 5 月 18 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDirectConnectServiceRolePolicy

AWSDirectConnectServiceRolePolicy 是一项 [AWS 托管策略](#)：提供代表您创建和管理 AWS 资源的 AWS Direct Connect 权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 1 月 14 日 18:35 UTC

- 编辑时间：2021 年 1 月 14 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDirectoryServiceFullAccess

AWSDirectoryServiceFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Directory Service 的完全访问权限。

使用此策略

您可以将 `AWSDirectoryServiceFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:41 UTC
- 编辑时间 : 2020 年 11 月 24 日 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDirectoryServiceReadOnlyAccess

AWSDirectoryServiceReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Directory Service 的只读访问权限。

使用此策略

您可以将 AWSDirectoryServiceReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2018 年 9 月 25 日 21:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDiscoveryContinuousExportFirehosePolicy

AWSDiscoveryContinuousExportFirehosePolicy 是一项 [AWS 托管策略](#)：提供对 AWS Discovery Continuous Export 所需 AWS 资源的写入权限

使用此策略

您可以将 `AWSDiscoveryContinuousExportFirehosePolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 8 月 9 日 18:29 UTC
- 编辑时间 : 2021 年 6 月 8 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDMSFleetAdvisorServiceRolePolicy

AWSDMSFleetAdvisorServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 DMS Fleet Advisor 代表您管理 CloudWatch 指标。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 6 日 09:10 UTC
- 编辑时间：2023 年 3 月 6 日 09:10 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSDMSServerlessServiceRolePolicy

AWSDMSServerlessServiceRolePolicy 是一项 [AWS 托管策略](#)：授予 AWS DMS Serverless 权限，允许代表您在账户中创建和管理 DMS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 5 月 18 日 20:28 UTC
- 编辑时间：2023 年 5 月 18 日 20:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEC2CapacityReservationFleetRolePolicy

AWSEC2CapacityReservationFleetRolePolicy 是一项 [AWS 托管策略](#)：允许 EC2 CapacityReservation Fleet 服务管理容量预留

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 29 日 14:43 UTC
- 编辑时间：2021 年 9 月 29 日 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEC2FleetServiceRolePolicy

AWSEC2FleetServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 EC2 Fleet 启动和管理实例。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 21 日 00:08 UTC
- 编辑时间：2020 年 5 月 4 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEC2SpotFleetServiceRolePolicy

AWSEC2SpotFleetServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 EC2 Spot Fleet 启动和管理竞价型实例集实例

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 23 日 19:13 UTC

- 编辑时间：2020 年 3 月 16 日 19:16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    ]
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEC2SpotServiceRolePolicy

AWSEC2SpotServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 EC2 Spot 启动和管理竞价型实例

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 18 日 18:51 UTC
- 编辑时间：2018 年 12 月 12 日 00:13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSECRPullThroughCache_ServiceRolePolicy

AWSECRPullThroughCache_ServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 AWS ECR 缓存提取使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 26 日 21:51 UTC
- 编辑时间：2023 年 11 月 13 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkCustomPlatformforEC2Role

AWSElasticBeanstalkCustomPlatformforEC2Role 是一项 [AWS 托管策略](#)：在您的自定义平台构建器环境中为实例提供启动 EC2 实例、创建 EBS 快照和 AMI、将日志流式传输到 Amazon CloudWatch Logs 以及在 Amazon S3 中存储构件的权限。

使用此策略

您可以将 AWSElasticBeanstalkCustomPlatformforEC2Role 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 2 月 21 日 22:50 UTC
- 编辑时间：2017 年 2 月 21 日 22:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkEnhancedHealth

AWSElasticBeanstalkEnhancedHealth 是一项 [AWS 托管策略](#)：适用于健康监控系统的 AWS Elastic Beanstalk 服务策略

使用此策略

您可以将 AWSElasticBeanstalkEnhancedHealth 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 8 日 23:17 UTC
- 编辑时间：2018 年 4 月 9 日 22:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkMaintenance

AWSElasticBeanstalkMaintenance 是一项 [AWS 托管策略](#)：AWS Elastic Beanstalk 服务角色策略，该策略授予有限的权限，允许代表您更新资源以进行维护。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 1 月 11 日 23:22 UTC
- 编辑时间：2019 年 6 月 4 日 17:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 是一项 [AWS 托管策略](#)：此策略适用于用来对 AWS Elastic Beanstalk 环境执行托管更新的 Elastic Beanstalk 服务角色。不应将此策略附加到其他用户或角色。该策略授予了在包括 AutoScaling、EC2、ECS、Elastic Load Balancing 和

CloudFormation 在内的多种AWS服务中创建和管理资源的广泛权限。该策略还允许传递可与这些服务一起使用的任何 IAM 角色。

使用此策略

您可以将 `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2021 年 3 月 3 日 22:18 UTC
- 编辑时间 : 2023 年 3 月 23 日 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Elastic Beanstalk 服务角色策略，用于授予对托管更新的有限权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 21 日 22:35 UTC
- 编辑时间：2023 年 3 月 24 日 00:18 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkMulticontainerDocker

AWSElasticBeanstalkMulticontainerDocker 是一项 [AWS 托管策略](#)：为您的多容器 Docker 环境中的实例提供访问权限，使其能够使用 Amazon EC2 容器服务来管理容器部署任务。

使用此策略

您可以将 AWSElasticBeanstalkMulticontainerDocker 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:15 UTC
- 编辑时间：2023 年 3 月 23 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkReadOnly

AWSElasticBeanstalkReadOnly 是一项 [AWS 托管策略](#)：授予只读权限。明确允许操作人员获取直接访问权限，以检索与 AWS Elastic Beanstalk 应用程序相关资源的信息。

使用此策略

您可以将 AWSElasticBeanstalkReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 19:02 UTC
- 编辑时间：2021 年 1 月 22 日 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleCore

AWSElasticBeanstalkRoleCore 是一项 [AWS 托管策略](#)：

AWSElasticBeanstalkRoleCore (Elastic Beanstalk 操作角色) 允许 Web 服务环境的核心操作。

使用此策略

您可以将 AWSElasticBeanstalkRoleCore 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:48 UTC
- 编辑时间：2020 年 9 月 9 日 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "S30bj",
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleCWL

AWSElasticBeanstalkRoleCWL 是一项 [AWS 托管策略](#) : (Elastic Beanstalk 操作角色) 允许环境管理 Amazon CloudWatch Logs 日志组。

使用此策略

您可以将 AWSElasticBeanstalkRoleCWL 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:49 UTC
- 编辑时间：2020 年 6 月 5 日 21:49 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs>DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleECS

AWSElasticBeanstalkRoleECS 是一项 [AWS 托管策略](#)：(Elastic Beanstalk 操作角色) 允许多容器 Docker 环境管理 Amazon ECS 集群。

使用此策略

您可以将 AWSElasticBeanstalkRoleECS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:47 UTC
- 编辑时间：2023 年 3 月 23 日 22:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleRDS

AWSElasticBeanstalkRoleRDS 是一项 [AWS 托管策略](#)：(Elastic Beanstalk 操作角色) 允许环境集成 Amazon RDS 实例。

使用此策略

您可以将 AWSElasticBeanstalkRoleRDS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:46 UTC

- 编辑时间：2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleSNS

AWSElasticBeanstalkRoleSNS 是一项 [AWS 托管策略](#)：(Elastic Beanstalk 操作角色) 允许环境启用 Amazon SNS 主题集成。

使用此策略

您可以将 AWSElasticBeanstalkRoleSNS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:46 UTC
- 编辑时间：2020 年 6 月 5 日 21:46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkRoleWorkerTier

AWSElasticBeanstalkRoleWorkerTier 是一项 [AWS 托管策略](#)：(Elastic Beanstalk 操作角色) 允许工作线程环境层创建 Amazon DynamoDB 表和 Amazon SQS 队列。

使用此策略

您可以将 AWSElasticBeanstalkRoleWorkerTier 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 6 月 5 日 21:43 UTC
- 编辑时间：2020 年 6 月 5 日 21:43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkService

AWSElasticBeanstalkService 是一项 [AWS 托管策略](#)：此策略很快将被弃用。有关指南，请参阅文档：<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html>。AWSElastic Beanstalk 服务角色策略，授予代表您创建和管理资源（即：AutoScaling、EC2、S3、CloudFormation、ELB 等）的权限。

使用此策略

您可以将 AWSElasticBeanstalkService 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 4 月 11 日 20:27 UTC
- 编辑时间：2023 年 5 月 10 日 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

策略版本

策略版本：v17（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkServiceRolePolicy

AWSElasticBeanstalkServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Elastic Beanstalk 服务相关角色策略，授予代表您创建和管理资源（即：AutoScaling、EC2、S3、CloudFormation、ELB 等）的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 13 日 23:46 UTC
- 编辑时间：2019 年 6 月 6 日 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

策略版本

策略版本：v6（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkWebTier

AWSElasticBeanstalkWebTier 是一项 [AWS 托管策略](#)：向您的 Web 服务器环境中的实例提供将日志文件上传到 Amazon S3 的访问权限。

使用此策略

您可以将 AWSElasticBeanstalkWebTier 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:08 UTC
- 编辑时间：2020 年 9 月 9 日 19:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticBeanstalkWorkerTier

AWSElasticBeanstalkWorkerTier 是一项 [AWS 托管策略](#)：向您工作线程环境中的实例提供访问权限，用以将日志文件上传到 Amazon S3、使用 Amazon SQS 监控应用程序的任务队列、使用 Amazon DynamoDB 进行领导选择以及使用 Amazon CloudWatch 发布运行状况监控指标。

使用此策略

您可以将 AWSElasticBeanstalkWorkerTier 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 2 月 8 日 23:12 UTC
- 编辑时间：2020 年 9 月 9 日 19:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryAgentInstallationPolicy

AWSElasticDisasterRecoveryAgentInstallationPolicy 是一项 [AWS 托管策略](#)：此策略允许安装 AWS Replication Agent，它与 AWS Elastic Disaster Recovery (DRS) 结合使用，用于将外部服务器恢复至 AWS。可将此策略附加到您在 AWS Replication Agent 安装步骤中提供凭证的 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryAgentInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:37 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 12:38
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryAgentInstallationPolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryAgentPolicy

AWSElasticDisasterRecoveryAgentPolicy 是一项 [AWS 托管策略](#)：此策略允许使用 AWS Replication Agent，它与 AWS Elastic Disaster Recovery (DRS) 结合使用，用于将源服务器恢复至 AWS。我们不建议您将此策略附加到 IAM 用户或角色。

使用此策略

您可以将 `AWSElasticDisasterRecoveryAgentPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:32 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:44
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryConsoleFullAccess

AWSElasticDisasterRecoveryConsoleFullAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS Elastic Disaster Recovery (DRS) 所有公共 API 的完全访问权限，以及读取 KMS 密钥、License Manager、Resource Groups、弹性负载均衡器、IAM 和 EC2 信息的权限。可将此策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:46 UTC
- 编辑时间：2023 年 10 月 16 日 12:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryConsoleFullAccess_v2

AWSElasticDisasterRecoveryConsoleFullAccess_v2是一项[AWS托管策略](#)：该策略提供对AWS Elastic 灾难恢复 (AWSDRS) 的所有公共 API 以及 DRS 控制台使用的其他AWS服务中的所有公共 API 的AWS完全访问权限。将此策略附加到您的用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryConsoleFullAccess_v2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 27 日 13:35
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:35
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryConsoleFullAccess_v2

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
    "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/
AWS_ElasticDisasterRecoveryConversionServerRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceRole",
      "arn:aws:iam::*:role/service-role/
AWS_ElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
    ],
    "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"
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryConversionServerPolicy

AWSElasticDisasterRecoveryConversionServerPolicy 是一项 [AWS 托管策略](#)：此策略附加到 AWS Elastic Disaster Recovery 转换服务器的实例角色。此策略允许 Elastic Disaster Recovery (DRS) 转换服务器 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务进行通信。DRS 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 DRS 转换服务器 (由 DRS 在需要时自动启动和终止)。我们不建议您将此策略附加到 IAM 用户或角色。当用户选择使用 DRS 控制台、CLI 或 API 恢复源服务器时，Elastic Disaster Recovery 会使用 DRS 转换服务器。

使用此策略

您可以将 AWSElasticDisasterRecoveryConversionServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 13:42 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:13
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 是一项 [AWS 托管策略](#)：此策略允许 AWS Elastic Disaster Recovery (DRS) 支持跨账户复制和跨账户失效自动恢复。

使用此策略

您可以将 AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 5 月 14 日 07:16 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 13:19
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryEc2InstancePolicy

AWSElasticDisasterRecoveryEc2InstancePolicy 是一项 [AWS 托管策略](#)：此策略允许安装和使用 AWS 复制代理，AWS Elastic Disaster Recovery (DRS) 使用该代理来恢复在 EC2 (跨区域或跨可用区) 上运行的源服务器。应将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 EC2 实例。

使用此策略

您可以将 AWSElasticDisasterRecoveryEc2InstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2022 年 5 月 26 日 12:30 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:39
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryFailbackInstallationPolicy

AWSElasticDisasterRecoveryFailbackInstallationPolicy 是一个 [AWS 托管策略](#)，它：您可以将该 AWSElasticDisasterRecoveryFailbackInstallationPolicy 策略附加到您的 IAM 身份。此策略允许安装 Elastic Disaster Recovery 失效自动恢复客户端，该客户端用于将恢复实例失效自动恢复到原始源基础设施。可将此策略附加到您在运行 Elastic Disaster Recovery 失效自动恢复客户端时提供凭证的 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryFailbackInstallationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 11:02 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:43
- ARN: arn:aws:iam::aws:policy/
AWSElasticDisasterRecoveryFailbackInstallationPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryFailbackPolicy

AWSElasticDisasterRecoveryFailbackPolicy 是一项 [AWS 托管策略](#)：此策略允许使用 Elastic Disaster Recovery 失效自动恢复客户端，该客户端用于将恢复实例失效自动恢复到原始源基础设施。我们不建议您将此策略附加到 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryFailbackPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:41 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 12:56
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryLaunchActionsPolicy

AWSElasticDisasterRecoveryLaunchActionsPolicy 是一项 [AWS 托管策略](#)：此策略允许您使用 Amazon SSM 以及其他服务，并授予所需的权限，以便在 AWS Elastic Disaster Recovery (AWS DRS) 中执行启动后操作。将此策略附加到您的 IAM 角色或用户。

使用此策略

您可以将 AWSElasticDisasterRecoveryLaunchActionsPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 9 月 13 日 07:38 UTC
- 编辑时间：2023 年 10 月 16 日 12:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AWSDistro0Tel-*",
  "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/AWSDistro0Tel-*:*",
"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"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryNetworkReplicationPolicy

AWSElasticDisasterRecoveryNetworkReplicationPolicy 是一项 [AWS 托管策略](#)：此策略允许 AWS Elastic Disaster Recovery (DRS) 支持网络复制。

使用此策略

您可以将 AWSElasticDisasterRecoveryNetworkReplicationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 11 日 12:36 UTC
- 编辑时间：世界标准时间 2024 年 1 月 2 日 13:25
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryReadOnlyAccess

AWSElasticDisasterRecoveryReadOnlyAccess 是一个 [AWS 托管策略](#)，它：您可以将该 AWSElasticDisasterRecoveryReadOnlyAccess 策略附加到您的 IAM 身份。此策略提供对以下 API 的权限：Elastic Daser Recovery (DRS) 的所有只读公共 API，以及为了完全只读使用 DRS 控制台所需的其他 AWS 服务的一些只读 API。可将此策略附加到您的 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 17 日 10:50 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:03
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryRecoveryInstancePolicy

AWSElasticDisasterRecoveryRecoveryInstancePolicy 是一项 [AWS 托管策略](#)：此策略附加到 Elastic Disaster Recovery 的恢复实例的实例角色。此策略允许 Elastic Disaster Recovery (DRS) 恢复实例 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务通信，并能够对其原始源基础设施执行失效自动恢复。Elastic Disaster Recovery 将具有此策略的 IAM 角色 (作为 EC2 实例配置文件) 附加到 DRS 恢复实例。我们不建议您将此策略附加到 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryRecoveryInstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 11 月 17 日 10:20 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:11
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryReplicationServerPolicy

AWSElasticDisasterRecoveryReplicationServerPolicy 是一项 [AWS 托管策略](#)：

此策略附加到 Elastic Disaster Recovery 复制服务器的实例角色。此策略允许 Elastic Disaster Recovery (DRS) 复制服务器 (由 Elastic Disaster Recovery 启动的 EC2 实例) 与 DRS 服务进行通信，并在您的 AWS 账户中创建 EBS 快照。Elastic Disaster Recovery 将具有此策略的 IAM 角色 (作

为 EC2 实例配置文件) 附加到 DRS 复制服务器 (由 DRS 在需要时自动启动和终止)。在 DRS 托管的恢复过程中 , DRS 复制服务器用于加快从外部服务器到 AWS 的数据复制。我们不建议您将此策略附加到 IAM 用户或角色。

使用此策略

您可以将 `AWSElasticDisasterRecoveryReplicationServerPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型 : 服务角色策略
- 创建时间 : 2021 年 11 月 17 日 13:34 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 27 日 13:28
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时 , AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryServiceRolePolicy

AWSElasticDisasterRecoveryServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略允许 Elastic Disaster Recovery 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 17 日 10:56 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 13:49
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryStagingAccountPolicy

AWSElasticDisasterRecoveryStagingAccountPolicy 是一项 [AWS 托管策略](#)：此策略允许对 AWS Elastic Disaster Recovery (DRS) 资源 (例如源服务器和作业) 进行只读访问。它还允许创建一个转换后的快照并与特定账户共享该 EBS 快照。

使用此策略

您可以将 AWSElasticDisasterRecoveryStagingAccountPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 5 月 26 日 09:49 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 13:07
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 是一项 [AWS 托管策略](#) : AWS Elastic Disaster Recovery (DRS) 使用此策略将源服务器恢复到单独的目标账户中并允许失效自动恢复。我们不建议您将此策略附加到 IAM 用户或角色。

使用此策略

您可以将 AWSElasticDisasterRecoveryStagingAccountPolicy_v2 附加到您的用户、组和角色。

策略详细信息

- 类型 : 服务角色策略
- 创建时间 : 2023 年 1 月 5 日 12:11 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 27 日 13:32
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时 , AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticLoadBalancingClassicServiceRolePolicy

AWSElasticLoadBalancingClassicServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS 弹性负载均衡器控制面板经典版的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 19 日 22:36 UTC
- 编辑时间：2019 年 10 月 7 日 23:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElasticLoadBalancingServiceRolePolicy

AWSElasticLoadBalancingServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS 弹性负载均衡器控制面板的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 19 日 22:19 UTC
- 编辑时间：2021 年 8 月 26 日 19:01 UTC

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

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaConvertFullAccess

AWSElementalMediaConvertFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 AWS Elemental MediaConvert 的完全访问权限。

使用此策略

您可以将 AWSElementalMediaConvertFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 25 日 19:25 UTC
- 编辑时间：2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaConvertReadOnly

AWSElementalMediaConvertReadOnly 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 AWS Elemental MediaConvert 的只读访问权限。

使用此策略

您可以将 AWSElementalMediaConvertReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 25 日 19:25 UTC
- 编辑时间：2019 年 6 月 10 日 22:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",

```

```
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaLiveFullAccess

AWSElementalMediaLiveFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaLive 资源的完全访问权限

使用此策略

您可以将 AWSElementalMediaLiveFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 8 日 17:07 UTC
- 编辑时间：2020 年 7 月 8 日 17:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaLiveReadOnly

AWSElementalMediaLiveReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaLive 资源的只读访问权限

使用此策略

您可以将 AWSElementalMediaLiveReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 7 月 8 日 16:38 UTC
- 编辑时间：2020 年 7 月 8 日 16:38 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaPackageFullAccess

AWSElementalMediaPackageFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaPackage 资源的完全访问权限

使用此策略

您可以将 AWSElementalMediaPackageFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 12 月 29 日 23:39 UTC

- 编辑时间：2017 年 12 月 29 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaPackageReadOnly

AWSElementalMediaPackageReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaPackage 资源的只读访问权限

使用此策略

您可以将 AWSElementalMediaPackageReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 12 月 30 日 00:04 UTC
- 编辑时间 : 2017 年 12 月 30 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaPackageV2FullAccess

AWSElementalMediaPackageV2FullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaPackageV2 资源的完全访问权限。

使用此策略

您可以将 AWSElementalMediaPackageV2FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 20:29 UTC
- 编辑时间：2023 年 7 月 25 日 20:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaPackageV2ReadOnly

AWSElementalMediaPackageV2ReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaPackageV2 资源的只读访问权限。

使用此策略

您可以将 AWSElementalMediaPackageV2ReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 20:31 UTC
- 编辑时间：2023 年 7 月 25 日 20:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediapackagev2:List*",
        "mediapackagev2:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaStoreFullAccess

AWSElementalMediaStoreFullAccess 是一项 [AWS 托管策略](#)：提供对所有 MediaStore API 的完全读取和写入权限

使用此策略

您可以将 AWSElementalMediaStoreFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 5 日 23:15 UTC
- 编辑时间：2018 年 3 月 5 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "mediastore:*"
    ],
    "Effect" : "Allow",
    "Resource" : "*",
    "Condition" : {
      "Bool" : {
        "aws:SecureTransport" : "true"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaStoreReadOnly

AWSElementalMediaStoreReadOnly 是一项 [AWS 托管策略](#)：为 MediaStore API 提供只读权限

使用此策略

您可以将 AWSElementalMediaStoreReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 8 日 19:48 UTC
- 编辑时间：2018 年 3 月 8 日 19:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaTailorFullAccess

AWSElementalMediaTailorFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaTailor 资源的完全访问权限

使用此策略

您可以将 AWSElementalMediaTailorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 23 日 00:04 UTC
- 编辑时间：2021 年 11 月 23 日 00:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSElementalMediaTailorReadOnly

AWSElementalMediaTailorReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Elemental MediaTailor 资源的只读访问权限

使用此策略

您可以将 AWSElementalMediaTailorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 23 日 00:05 UTC
- 编辑时间：2021 年 11 月 23 日 00:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEnhancedClassicNetworkingMangementPolicy

AWSEnhancedClassicNetworkingMangementPolicy是一项 [AWS 托管策略](#)：用于启用增强型经典网络管理功能的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 9 月 20 日 17:29 UTC
- 编辑时间：2017 年 9 月 20 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "ec2:DescribeInstances",
      "ec2:DescribeSecurityGroups"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEntityResolutionConsoleFullAccess

AWSEntityResolutionConsoleFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Entity Resolution 和相关服务的控制台完全访问权限。

使用此策略

您可以将 AWSEntityResolutionConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 17 日 17:54 UTC
- 编辑时间：2023 年 10 月 16 日 18:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSEntityResolutionConsoleReadOnlyAccess

AWSEntityResolutionConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Entity Resolution 的只读访问权限。

使用此策略

您可以将 AWSEntityResolutionConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 17 日 18:18 UTC
- 编辑时间：2023 年 8 月 17 日 18:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorEC2Access

AWSFaultInjectionSimulatorEC2Access 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 EC2 和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:39 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 15:08
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorECSAccess

AWSFaultInjectionSimulatorECSAccess 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 ECS 和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorECSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:37 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 16:16
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorEKSAccess

AWSFaultInjectionSimulatorEKSAccess 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 EKS 和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorEKSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:34 UTC
- 编辑时间：2023 年 11 月 13 日 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorNetworkAccess

AWSFaultInjectionSimulatorNetworkAccess 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 EC2 网络和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorNetworkAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 20:32 UTC
- 编辑时间：世界标准时间 2024 年 1 月 25 日 16:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorRDSAccess

AWSFaultInjectionSimulatorRDSAccess 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 RDS 和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorRDSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2022 年 10 月 26 日 20:30 UTC
- 编辑时间：2023 年 11 月 13 日 16:23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFaultInjectionSimulatorSSMAccess

AWSFaultInjectionSimulatorSSMAccess 是一项 [AWS 托管策略](#)：此策略授予 Fault Injection Simulator 服务在 SSM 和其他必需服务中执行 FIS 操作的权限。

使用此策略

您可以将 AWSFaultInjectionSimulatorSSMAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 10 月 26 日 15:33 UTC
- 编辑时间：2023 年 6 月 2 日 22:55 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFinSpaceServiceRolePolicy

AWSFinSpaceServiceRolePolicy 是一项 [AWS 托管策略](#)，它具有：允许访问亚马逊使用或管理的资源 AWS 服务以及允许访问亚马逊使用或管理的资源的策略 FinSpace

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2023 年 5 月 12 日 16:42 UTC
- 编辑时间：世界标准时间 2023 年 12 月 1 日 21:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFMAdminFullAccess

AWSFMAdminFullAccess 是一项 [AWS 托管策略](#)：AWS FM 管理员的完全访问权限

使用此策略

您可以将 AWSFMAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 9 日 18:06 UTC
- 编辑时间：2022 年 10 月 20 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFMAdminReadOnlyAccess

AWSFMAdminReadOnlyAccess 是一项 [AWS 托管策略](#)：对 AWS FM 管理员的只读访问权限，允许监控 AWS FM 操作

使用此策略

您可以将 AWSFMAdminReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 9 日 20:07 UTC
- 编辑时间：2022 年 10 月 31 日 22:42 UTC
- ARN: arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSFMMemberReadOnlyAccess

AWSFMMemberReadOnlyAccess 是一项 [AWS 托管策略](#)：为 AWS Firewall Manager 成员账户提供对 AWS WAF 操作的只读访问权限

使用此策略

您可以将 `AWSFMMemberReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 5 月 9 日 21:05 UTC
- 编辑时间 : 2018 年 5 月 9 日 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSForWordPressPluginPolicy

AWSForWordPressPluginPolicy 是一项 [AWS 托管策略](#)：适用于 Wordpress 的 AWS 插件的托管策略

使用此策略

您可以将 AWSForWordPressPluginPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 30 日 00:27 UTC
- 编辑时间：2020 年 1 月 20 日 23:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGitSyncServiceRolePolicy

AWSGitSyncServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Code Connections 从您的 Git 存储库中同步内容的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 16 日 17:05 UTC
- 编辑时间：2023 年 11 月 16 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlobalAcceleratorSLRPolicy

AWSGlobalAcceleratorSLRPolicy 是一项 [AWS 托管策略](#)：向 AWS Global Accelerator 授予管理 EC2 弹性网络接口和安全组的权限的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 4 月 5 日 19:39 UTC
- 编辑时间：2023 年 9 月 12 日 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueConsoleFullAccess

AWSGlueConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Glue 的完全访问权限。

使用此策略

您可以将 AWSGlueConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 7 月 14 日 14:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueConsoleSageMakerNotebookFullAccess

AWSGlueConsoleSageMakerNotebookFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Glue 的完全访问权限和对 SageMaker 笔记本实例的访问权限。

使用此策略

您可以将 AWSGlueConsoleSageMakerNotebookFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 5 日 17:52 UTC
- 编辑时间：2021 年 7 月 15 日 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AwsGlueDataBrewFullAccessPolicy

AwsGlueDataBrewFullAccessPolicy 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Glue DataBrew 的完全访问权限。同时，还提供对相关服务（例如 S3、KMS、Glue）的部分访问权限。

使用此策略

您可以将 AwsGlueDataBrewFullAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 11 日 16:51 UTC
- 编辑时间：2022 年 2 月 4 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy

策略版本

策略版本：v8（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueDataBrewServiceRole

AWSGlueDataBrewServiceRole 是一项 [AWS 托管策略](#)：此策略授予 Glue 对用户的 Glue 数据目录执行操作的权限，此策略还提供 EC2 操作权限，允许 Glue 创建 ENI 以连接到 VPC 中的资源，还允许 Glue 访问 LakeFormation 中的注册数据以及访问用户的 CloudWatch

使用此策略

您可以将 AWSGlueDataBrewServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 4 日 21:26 UTC
- 编辑时间：世界标准时间 2024 年 3 月 20 日 23:28
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSGlueSchemaRegistryFullAccess

AWSGlueSchemaRegistryFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Glue 架构注册表服务的完全访问权限

使用此策略

您可以将 AWSGlueSchemaRegistryFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 00:19 UTC

- 编辑时间：2020 年 11 月 20 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueSchemaRegistryReadOnlyAccess

AWSGlueSchemaRegistryReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Glue 架构注册表服务的只读访问权限

使用此策略

您可以将 AWSGlueSchemaRegistryReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 20 日 00:20 UTC
- 编辑时间：2020 年 11 月 20 日 00:20 UTC

- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueServiceNotebookRole

AWSGlueServiceNotebookRole 是一项 [AWS 托管策略](#)：面向 AWS Glue 服务角色的策略，允许客户管理笔记本服务器

使用此策略

您可以将 AWSGlueServiceNotebookRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 10 月 9 日 15:59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGlueServiceRole

AWSGlueServiceRole 是一项 [AWS 托管策略](#)：面向 AWS Glue 服务角色的策略，允许访问相关服务（包括 EC2、S3 和 Cloudwatch Logs）

使用此策略

您可以将 AWSGlueServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:37 UTC
- 编辑时间：2023 年 9 月 11 日 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

策略版本

策略版本：v5（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AwsGlueSessionUserRestrictedNotebookPolicy

AwsGlueSessionUserRestrictedNotebookPolicy 是一项 [AWS 托管策略](#)：提供允许用户仅创建和使用与用户关联的笔记本会话的权限。此策略还包括明确允许用户传递受限 Glue 会话角色的权限。

使用此策略

您可以将 AwsGlueSessionUserRestrictedNotebookPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 18 日 15:24 UTC
- 编辑时间：世界标准时间 2023 年 11 月 22 日 01:32
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AwsGlueSessionUserRestrictedNotebookServiceRole

AwsGlueSessionUserRestrictedNotebookServiceRole 是一项 [AWS 托管策略](#)：提供对除会话之外的所有 AWS Glue 资源的完全访问权限。允许用户仅创建和使用与用户关联的笔记本会话。此策略还包括 AWS Glue 管理其他 AWS 服务中的 Glue 资源所需的其他权限。

使用此策略

您可以将 AwsGlueSessionUserRestrictedNotebookServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 18 日 15:27 UTC
- 编辑时间：2022 年 4 月 18 日 15:27 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AwsGlueSessionUserRestrictedPolicy

AwsGlueSessionUserRestrictedPolicy 是一项 [AWS 托管策略](#)：提供允许用户仅创建和使用与用户关联的交互式会话的权限。此策略还包括明确允许用户传递受限 Glue 会话角色的权限。

使用此策略

您可以将 AwsGlueSessionUserRestrictedPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 14 日 21:31 UTC
- 编辑时间：2022 年 4 月 14 日 21:31 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:user}"
        }
      },
    }
  ]
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AwsGlueSessionUserRestrictedServiceRole

AwsGlueSessionUserRestrictedServiceRole 是一项 [AWS 托管策略](#)：提供对除会话之外的所有 AWS Glue 资源的完全访问权限。允许用户仅创建和使用与用户关联的交互式会话。此策略还包括 AWS Glue 管理其他 AWS 服务中的 Glue 资源所需的其他权限

使用此策略

您可以将 AwsGlueSessionUserRestrictedServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2022 年 4 月 14 日 21:30 UTC
- 编辑时间：2022 年 4 月 14 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGrafanaAccountAdministrator

AWSGrafanaAccountAdministrator 是一项 [AWS 托管策略](#)：提供在 Amazon Grafana 中为整个组织创建和管理工作区的访问权限。

使用此策略

您可以将 AWSGrafanaAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 23 日 00:20 UTC
- 编辑时间：2022 年 2 月 15 日 22:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGrafanaConsoleReadOnlyAccess

AWSGrafanaConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：访问 Amazon Grafana 中的只读操作。

使用此策略

您可以将 AWSGrafanaConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 23 日 00:10 UTC
- 编辑时间：2022 年 2 月 15 日 22:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
    "Effect" : "Allow",
    "Action" : [
      "grafana:Describe*",
      "grafana:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGrafanaWorkspacePermissionManagement

AWSGrafanaWorkspacePermissionManagement 是一项 [AWS 托管策略](#)：仅提供更新 AWS Grafana 工作区的用户和组权限的功能。

使用此策略

您可以将 AWSGrafanaWorkspacePermissionManagement 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 23 日 00:15 UTC
- 编辑时间：2023 年 3 月 15 日 22:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGrafanaWorkspacePermissionManagementV2

AWSGrafanaWorkspacePermissionManagementV2 是一项 [AWS 托管策略](#)，它：提供更新亚马逊托管 Grafana 工作空间的 IAM 身份中心 (IdC) 用户和群组权限的功能。

使用此策略

您可以将 AWSGrafanaWorkspacePermissionManagementV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2024 年 1 月 5 日 18:39
- 编辑时间：世界标准时间 2024 年 1 月 5 日 18:39
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGreengrassFullAccess

AWSGreengrassFullAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS Greengrass 配置、管理和部署操作的完全访问权限

使用此策略

您可以将 `AWSGreengrassFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 5 月 3 日 00:47 UTC
- 编辑时间 : 2017 年 5 月 3 日 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGreengrassReadOnlyAccess

AWSGreengrassReadOnlyAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS Greengrass 配置、管理和部署操作的只读访问权限

使用此策略

您可以将 AWSGreengrassReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 30 日 16:01 UTC
- 编辑时间：2018 年 10 月 30 日 16:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGreengrassResourceAccessRolePolicy

AWSGreengrassResourceAccessRolePolicy 是一项 [AWS 托管策略](#)：AWS Greengrass 服务角色策略，允许访问相关服务（包括 AWS Lambda 和 AWS IoT 事物影子）。

使用此策略

您可以将 AWSGreengrassResourceAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 2 月 14 日 21:17 UTC
- 编辑时间：2018 年 11 月 14 日 00:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

策略版本

策略版本：v5（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSGroundStationAgentInstancePolicy

AWSGroundStationAgentInstancePolicy 是一项 [AWS 托管策略](#)：提供使用 AWS Ground Station 代理的数据流端点实例权限

使用此策略

您可以将 AWSGroundStationAgentInstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 29 日 15:23 UTC
- 编辑时间：2023 年 3 月 29 日 15:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSHealth_EventProcessorServiceRolePolicy

AWSHealth_EventProcessorServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Health 启用运行状况事件处理器功能。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2023 年 1 月 13 日 19:24 UTC
- 编辑时间：2023 年 1 月 13 日 19:24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSHealthFullAccess

AWSHealthFullAccess 是一项 [AWS 托管策略](#)：允许完全访问 AWS Health API、Notifications 和 Personal Health Dashboard

使用此策略

您可以将 AWSHealthFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 6 日 12:30 UTC
- 编辑时间：2020 年 11 月 16 日 18:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSHealthImagingFullAccess

AWSHealthImagingFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Health Imaging 服务的完全访问权限。

使用此策略

您可以将 AWSHealthImagingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 23:39 UTC
- 编辑时间：2023 年 7 月 25 日 23:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSHealthImagingReadOnlyAccess

AWSHealthImagingReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Health Imaging 服务的只读访问权限。

使用此策略

您可以将 AWSHealthImagingReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 7 月 25 日 23:40 UTC
- 编辑时间：2023 年 8 月 1 日 15:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIAMIdentityCenterAllowListForIdentityContext

AWSIAMIdentityCenterAllowListForIdentityContext 是一项 [AWS 托管策略](#)：提供以下操作列表：允许在 IAM Identity Center 身份上下文中担任的角色执行的操作。AWSSecurity Token Service (AWS STS) 会自动将此策略附加到担任的角色。身份上下文传递为 ProvidedContext。

使用此策略

您可以将 `AWSIAMIdentityCenterAllowListForIdentityContext` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 11 月 8 日 15:21 UTC
- 编辑时间：世界标准时间 2023 年 11 月 25 日 19:27
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIdentitySyncFullAccess

AWSIdentitySyncFullAccess 是一项 [AWS 托管策略](#)：授予 Identity Sync 服务的完全访问权限

使用此策略

您可以将 AWSIdentitySyncFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 3 月 23 日 23:29 UTC
- 编辑时间：2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIdentitySyncReadOnlyAccess

AWSIdentitySyncReadOnlyAccess 是一项 [AWS 托管策略](#)：授予对 Identity Sync 服务的只读访问权限

使用此策略

您可以将 AWSIdentitySyncReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 3 月 23 日 23:29 UTC
- 编辑时间：2022 年 3 月 23 日 23:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "arn::*:identity-sync::*:*/*/*"  
  }  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSImageBuilderFullAccess

AWSImageBuilderFullAccess 是一项 [AWS 托管策略](#)：提供对所有 AWS Image Builder 操作的完全访问权限以及对相关 AWS 服务的资源限定访问权限。

使用此策略

您可以将 AWSImageBuilderFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 20 日 18:25 UTC
- 编辑时间：2021 年 4 月 13 日 17:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSImageBuilderReadOnlyAccess

AWSImageBuilderReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 AWS Image Builder 操作的只读访问权限。

使用此策略

您可以将 `AWSImageBuilderReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 12 月 19 日 22:29 UTC
- 编辑时间 : 2019 年 12 月 19 日 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSImportExportFullAccess

AWSImportExportFullAccess 是一项 [AWS 托管策略](#)：提供对在 AWS 账户下创建的作业的读取和写入权限。

使用此策略

您可以将 AWSImportExportFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "importexport:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSImportExportReadOnlyAccess

AWSImportExportReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对在 AWS 账户下创建的作业的只读访问权限。

使用此策略

您可以将 AWSImportExportReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIncidentManagerIncidentAccessServiceRolePolicy

AWSIncidentManagerIncidentAccessServiceRolePolicy 是一项 [AWS 托管策略](#)，它：授予事件管理员在管理事件时调用其他 AWS 服务的权限。

使用此策略

您可以将 AWSIncidentManagerIncidentAccessServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 11 月 13 日 00:01 UTC
- 编辑时间：世界标准时间 2024 年 2 月 20 日 23:02
- ARN: arn:aws:iam::aws:policy/
AWSIncidentManagerIncidentAccessServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSIncidentManagerResolverAccess

AWSIncidentManagerResolverAccess 是一项 [AWS 托管策略](#)：此策略授予启动、查看和更新事件的权限，以及对自定义时间表事件和相关项目的完全访问权限。可将此策略分配给将创建和解决事件的用户。

使用此策略

您可以将 AWSIncidentManagerResolverAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 5 月 10 日 06:12 UTC
- 编辑时间：2021 年 5 月 10 日 06:12 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIncidentManagerServiceRolePolicy

AWSIncidentManagerServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略授予 Incident Manager 代表您管理事件记录和相关资源的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 10 日 03:34 UTC
- 编辑时间：2022 年 12 月 5 日 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoT1ClickFullAccess

AWSIoT1ClickFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS IoT 1-Click 的完全访问权限。

使用此策略

您可以将 AWSIoT1ClickFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 5 月 11 日 22:10 UTC
- 编辑时间：2018 年 5 月 11 日 22:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iot1click:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoT1ClickReadOnlyAccess

AWSIoT1ClickReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS IoT 1-Click 的只读访问权限。

使用此策略

您可以将 `AWSIoT1ClickReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 11 日 21:49 UTC
- 编辑时间：2018 年 5 月 11 日 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTAnalyticsFullAccess

AWSIoTAnalyticsFullAccess 是一项 [AWS 托管策略](#)：提供对 IoT Analytics 的完全访问权限。

使用此策略

您可以将 AWSIoTAnalyticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 18 日 23:02 UTC
- 编辑时间：2018 年 6 月 18 日 23:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTAnalyticsReadOnlyAccess

AWSIoTAnalyticsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 IoT Analytics 的只读访问权限。

使用此策略

您可以将 AWSIoTAnalyticsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 18 日 21:37 UTC
- 编辑时间：2018 年 6 月 18 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

```
{
  "Effect" : "Allow",
  "Action" : [
    "iotanalytics:Describe*",
    "iotanalytics:List*",
    "iotanalytics:Get*",
    "iotanalytics:SampleChannelData"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTConfigAccess

AWSIoTConfigAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS IoT 配置操作的完全访问权限

使用此策略

您可以将 AWSIoTConfigAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 27 日 21:52 UTC
- 编辑时间：2019 年 9 月 27 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTConfigReadOnlyAccess

AWSIoTConfigReadOnlyAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS IoT 配置操作的只读访问权限

使用此策略

您可以将 AWSIoTConfigReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 27 日 21:52 UTC
- 编辑时间：2019 年 9 月 27 日 20:52 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDataAccess

AWSIoTDataAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS IoT 消息收发操作的完全访问权限

使用此策略

您可以将 AWSIoTDataAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 10 月 27 日 21:51 UTC
- 编辑时间 : 2021 年 6 月 23 日 21:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 是一项 [AWS 托管策略](#)：提供对 IoT 事物组的写入权限和对 IoT 证书的读取权限，以执行 ADD_THINGS_TO_THING_GROUP 缓解操作

使用此策略

您可以将 AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:55 UTC
- 编辑时间：2019 年 8 月 7 日 17:55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    "Effect" : "Allow",
    "Action" : [
      "iot:ListPrincipalThings",
      "iot:AddThingToThingGroup"
    ],
    "Resource" : [
      "*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderAudit

AWSIoTDeviceDefenderAudit 是一项 [AWS 托管策略](#)：提供对 IoT 和相关资源的读取权限

使用此策略

您可以将 AWSIoTDeviceDefenderAudit 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 7 月 18 日 21:17 UTC
- 编辑时间：2019 年 11 月 25 日 23:52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 是一项 [AWS 托管策略](#)：提供访问权限以启用 IoT 日志记录，用于执行 ENABLE_IOT_LOGGING 缓解操作

使用此策略

您可以将 AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC
- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : [
      "*"
    ]
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "iam:PassRole"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "StringEquals" : {
        "iam:PassedToService" : [
          "iot.amazonaws.com"
        ]
      }
    }
  }
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 是一项 [AWS 托管策略](#)：提供 SNS 主题的消息发布权限，用于执行 PUBLISH_FINDING_TO_SNS 缓解措施

使用此策略

您可以将 AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC
- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 是一项 [AWS 托管策略](#)：提供对 IoT 策略的写入权限，以执行 REPLACE_DEFAULT_POLICY_VERSION 缓解操作

使用此策略

您可以将 AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:04 UTC
- 编辑时间：2019 年 8 月 7 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderUpdateCACertMitigationAction

AWSIoTDeviceDefenderUpdateCACertMitigationAction 是一项 [AWS 托管策略](#)：提供对 IoT CA 证书的写入权限，以执行 UPDATE_CA_CERTIFICATE 缓解操作

使用此策略

您可以将 AWSIoTDeviceDefenderUpdateCACertMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:05 UTC
- 编辑时间：2019 年 8 月 7 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 是一项 [AWS 托管策略](#)：提供对 IoT CA 证书的写入权限，以执行 UPDATE_DEVICE_CERTIFICATE 缓解操作

使用此策略

您可以将 AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 8 月 7 日 17:06 UTC
- 编辑时间：2019 年 8 月 7 日 17:06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceTesterForFreeRTOSFullAccess

AWSIoTDeviceTesterForFreeRTOSFullAccess 是一项 [AWS 托管策略](#)：允许 AWS IoT Device Tester 通过允许访问包括 IoT、S3 和 IAM 在内的服务来运行 FreeRTOS 资格套件

使用此策略

您可以将 AWSIoTDeviceTesterForFreeRTOSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 2 月 12 日 20:33 UTC
- 编辑时间 : 2023 年 8 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTDeviceTesterForGreengrassFullAccess

AWSIoTDeviceTesterForGreengrassFullAccess 是一项 [AWS 托管策略](#)：允许 AWS IoT Device Tester 通过允许访问包括 Lambda、IoT、API Gateway 和 IAM 在内的相关服务来运行 AWS Greengrass 资格套件

使用此策略

您可以将 AWSIoTDeviceTesterForGreengrassFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2020 年 2 月 20 日 21:21 UTC
- 编辑时间：2020 年 6 月 25 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTEventsFullAccess

AWSIoTEventsFullAccess 是一项 [AWS 托管策略](#)：提供对 IoT Events 的完全访问权限。

使用此策略

您可以将 AWSIoTEventsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 10 日 22:51 UTC
- 编辑时间：2019 年 1 月 10 日 22:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTEventsReadOnlyAccess

AWSIoTEventsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 IoT Events 的只读访问权限。

使用此策略

您可以将 AWSIoTEventsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 10 日 22:50 UTC
- 编辑时间：2019 年 9 月 23 日 17:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoT FleetHubFederationAccess

AWSIoT FleetHubFederationAccess 是一项 [AWS 托管策略](#)：对 IoT Fleet Hub 应用程序的联合身份验证访问权限

使用此策略

您可以将 AWSIoT FleetHubFederationAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 15 日 08:08 UTC
- 编辑时间：2022 年 4 月 4 日 18:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoT FleetHubFederationAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoT FleetwiseServiceRolePolicy

AWSIoT FleetwiseServiceRolePolicy 是一项 [AWS 托管策略](#)：授予对 AWSIoT Fleetwise 使用或托管的用于辅助功能的 AWS 资源和元数据的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 9 月 21 日 23:27 UTC
- 编辑时间：2022 年 9 月 21 日 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoT FleetwiseServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTFullAccess

AWSIoTFullAccess 是一项 [AWS 托管策略](#)：此策略提供对 AWS IoT 配置和消息收发操作的完全访问权限

使用此策略

您可以将 AWSIoTFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 8 日 15:19 UTC
- 编辑时间：2022 年 5 月 19 日 21:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTLogging

AWSIoTLogging 是一项 [AWS 托管策略](#)：允许创建 Amazon CloudWatch 日志组并将日志流式传输到这些组

使用此策略

您可以将 AWSIoTLogging 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 10 月 8 日 15:17 UTC
- 编辑时间：2015 年 10 月 8 日 15:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs>DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTOTAUpdate

AWSIoTOTAUpdate 是一项 [AWS 托管策略](#)：允许创建 AWS IoT 作业并描述 AWS 代码签名作业

使用此策略

您可以将 AWSIoTOTAUpdate 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 12 月 20 日 20:36 UTC
- 编辑时间：2017 年 12 月 20 日 20:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTRoboRunnerFullAccess

AWSIoTRoboRunnerFullAccess 是一项 [AWS 托管策略](#)：此策略授予允许完全访问 AWS IoT RoboRunner 的权限。

使用此策略

您可以将 AWSIoTRoboRunnerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 03:54 UTC
- 编辑时间：2023 年 2 月 23 日 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTRoboRunnerFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTRoboRunnerReadOnly

AWSIoTRoboRunnerReadOnly 是一项 [AWS 托管策略](#)：此策略授予允许只读访问 AWS IoT RoboRunner 的权限。

使用此策略

您可以将 AWSIoTRoboRunnerReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2021 年 11 月 29 日 03:43 UTC
- 编辑时间：2022 年 11 月 16 日 20:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTRoboRunnerReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTRoboRunnerServiceRolePolicy

AWSIoTRoboRunnerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS IoT RoboRunner 代表客户管理关联的 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 2 月 21 日 16:56 UTC
- 编辑时间：2023 年 2 月 21 日 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTRoboRunnerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
    }  
  }  
}  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTRuleActions

AWSIoTRuleActions 是一项 [AWS 托管策略](#)：允许访问 AWS IoT 规则操作中支持的所有 AWS 服务

使用此策略

您可以将 AWSIoTRuleActions 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 10 月 8 日 15:14 UTC
- 编辑时间：2018 年 1 月 16 日 19:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTSiteWiseConsoleFullAccess

AWSIoTSiteWiseConsoleFullAccess 是一项 [AWS 托管策略](#)：提供使用 AWS Management Console 管理 AWS IoT SiteWise 的完全访问权限。请注意，此策略还授予以下权限：创建并列出与 AWS IoT SiteWise 一起使用的数据存储（例如 AWS IoT Analytics）、列出并查看 IoT AWS Greengrass 资源、列出并修改 AWS Secrets Manager 密钥、检索 AWS IoT 事物影子、列出带有特定标签的资源，以及为 AWS IoT SiteWise 创建并使用服务相关角色。

使用此策略

您可以将 AWSIoTSiteWiseConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 5 月 31 日 21:37 UTC

- 编辑时间：2019 年 5 月 31 日 21:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup"
  ],
  "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"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTSiteWiseFullAccess

AWSIoTSiteWiseFullAccess 是一项 [AWS 托管策略](#)：提供对 IoT SiteWise 的完全访问权限。

使用此策略

您可以将 AWSIoTSiteWiseFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 4 日 20:53 UTC
- 编辑时间：2018 年 12 月 4 日 20:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTSiteWiseMonitorPortalAccess

AWSIoTSiteWiseMonitorPortalAccess 是一项 [AWS 托管策略](#)：此策略授予以下权限：访问 AWS IoT SiteWise 资产和资产数据、创建 AWS IoT SiteWise Monitor 资源，以及列出 AWS SSO 用户。

使用此策略

您可以将 AWSIoTSiteWiseMonitorPortalAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 5 月 19 日 20:01 UTC

- 编辑时间：2020 年 5 月 19 日 20:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTSiteWiseMonitorServiceRolePolicy

AWSIoTSiteWiseMonitorServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略向 AWS IoT SiteWise 监视器授予权限，允许其访问您的 AWS IoT SiteWise 资产和资产属性，以及通过 AWS IoT SiteWise 门户创建 AWS IoT SiteWise 项目、控制面板和访问策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 14 日 00:59 UTC
- 编辑时间：2019 年 12 月 13 日 22:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTSiteWiseReadOnlyAccess

AWSIoTSiteWiseReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 IoT SiteWise 的只读访问权限。

使用此策略

您可以将 AWSIoTSiteWiseReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 12 月 4 日 20:55 UTC
- 编辑时间：2022 年 9 月 16 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotsitewise:Get*",
        "iotsitewise:BatchGet*"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTThingsRegistration

AWSIoTThingsRegistration 是一项 [AWS 托管策略](#)：此策略允许用户使用 AWS IoT StartThingRegistrationTask API 批量注册事物

使用此策略

您可以将 AWSIoTThingsRegistration 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 12 月 1 日 20:21 UTC
- 编辑时间：2020 年 10 月 5 日 19:20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTtwinMakerServiceRolePolicy

AWSIoTtwinMakerServiceRolePolicy是一项[AWS托管策略](#)：允许 AWS IoT TwinMaker 代表您调用其他AWS服务并同步其资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 13 日 18:59 UTC
- 编辑时间：2023 年 11 月 13 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTtwinMakerServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "IOTSITWISE"
      ]
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessDataAccess

AWSIoTWirelessDataAccess 是一项 [AWS 托管策略](#)：允许相关身份对 AWS IoT Wireless 设备进行数据访问。

使用此策略

您可以将 AWSIoTWirelessDataAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:31 UTC

- 编辑时间：2020 年 12 月 15 日 15:31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessFullAccess

AWSIoTWirelessFullAccess 是一项 [AWS 托管策略](#)：允许相关身份对所有 AWS IoT Wireless 操作进行完全访问。

使用此策略

您可以将 `AWSIoTWirelessFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:27 UTC
- 编辑时间：2020 年 12 月 15 日 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessFullPublishAccess

AWSIoTWirelessFullPublishAccess 是一项 [AWS 托管策略](#)：为 IoT Wireless 提供代表您发布到 IoT Rules Engine 的完全访问权限。

使用此策略

您可以将 AWSIoTWirelessFullPublishAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:29 UTC
- 编辑时间：2020 年 12 月 15 日 15:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessGatewayCertManager

AWSIoTWirelessGatewayCertManager 是一项 [AWS 托管策略](#)：授予相关身份访问权限，以创建、列出和描述 IoT 证书

使用此策略

您可以将 AWSIoTWirelessGatewayCertManager 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:30 UTC
- 编辑时间：2020 年 12 月 15 日 15:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Sid" : "IoTWirelessGatewayCertManager",
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateKeysAndCertificate",
      "iot:DescribeCertificate",
      "iot:ListCertificates"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessLogging

AWSIoTWirelessLogging 是一项 [AWS 托管策略](#)：允许相关身份创建 Amazon CloudWatch Logs 组以及将日志流式传输到这些组。

使用此策略

您可以将 AWSIoTWirelessLogging 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:32 UTC
- 编辑时间：2020 年 12 月 15 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessLogging

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIoTWirelessReadOnlyAccess

AWSIoTWirelessReadOnlyAccess 是一项 [AWS 托管策略](#)：允许相关身份对 AWS IoT Wireless 进行只读访问。

使用此策略

您可以将 `AWSIoTWirelessReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 15 日 15:28 UTC
- 编辑时间：2020 年 12 月 15 日 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSIPAMServiceRolePolicy

AWSIPAMServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 VPC IP 地址管理器代表您访问 VPC 资源并与 AWS Organizations 集成。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 30 日 19:08 UTC
- 编辑时间：2023 年 11 月 8 日 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIQContractServiceRolePolicy

AWSIQContractServiceRolePolicy 是一项 [AWS 托管策略](#)：由 AWS IQ 用来代表客户执行付款请求

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 22 日 19:28 UTC
- 编辑时间：2019 年 8 月 22 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIQFullAccess

AWSIQFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS IQ 的完全访问权限

使用此策略

您可以将 AWSIQFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 4 月 4 日 23:13 UTC
- 编辑时间：2019 年 9 月 25 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSIQPermissionServiceRolePolicy

AWSIQPermissionServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS IQ 管理由 AWS IQ 专家担任的角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 22 日 19:36 UTC
- 编辑时间：2019 年 8 月 22 日 19:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS KMS 自定义密钥存储所需的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 14 日 20:10 UTC
- 编辑时间：2023 年 11 月 10 日 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS KMS 同步多区域密钥的共享属性。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 16 日 15:37 UTC
- 编辑时间：2021 年 6 月 16 日 15:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSKeyManagementServicePowerUser

AWSKeyManagementServicePowerUser 是一项 [AWS 托管策略](#)：提供对 AWS Key Management Service (KMS) 的完全访问权限。

使用此策略

您可以将 AWSKeyManagementServicePowerUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2017 年 3 月 7 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLakeFormationCrossAccountManager

AWSLakeFormationCrossAccountManager 是一项 [AWS 托管策略](#)：提供通过 Lake Formation 对 Glue 资源的跨账户访问权限。同时，还授予对其他必需服务（例如组织和资源访问管理器）的读取权限

使用此策略

您可以将 AWSLakeFormationCrossAccountManager 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 4 日 20:59 UTC
- 编辑时间：2023 年 11 月 1 日 00:50 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLakeFormationDataAdmin

AWSLakeFormationDataAdmin 是一项 [AWS 托管策略](#)：授予对 AWS Lake Formation 和相关服务（例如 AWS Glue）的管理权限，以管理数据湖

使用此策略

您可以将 AWSLakeFormationDataAdmin 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2019 年 8 月 8 日 17:33 UTC
- 编辑时间 : 2019 年 12 月 16 日 22:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambda_FullAccess

AWSLambda_FullAccess 是一项 [AWS 托管策略](#)：授予对 AWS Lambda 服务、AWS Lambda 控制台功能和其他相关 AWS 服务的完全访问权限。

使用此策略

您可以将 AWSLambda_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 11 月 17 日 21:14 UTC
- 编辑时间 : 2020 年 11 月 17 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_FullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambda_ReadOnlyAccess

AWSLambda_ReadOnlyAccess 是一项 [AWS 托管策略](#)：授予对 AWS Lambda 服务、AWS Lambda 控制台功能和其他相关 AWS 服务的只读访问权限。

使用此策略

您可以将 `AWSLambda_ReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 11 月 17 日 21:10 UTC
- 编辑时间 : 2023 年 7 月 27 日 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaBasicExecutionRole

AWSLambdaBasicExecutionRole 是一项 [AWS 托管策略](#)：提供对 CloudWatch Logs 的写入权限。

使用此策略

您可以将 AWSLambdaBasicExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:03 UTC
- 编辑时间：2015 年 4 月 9 日 15:03 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaDynamoDBExecutionRole

AWSLambdaDynamoDBExecutionRole 是一项 [AWS 托管策略](#)：提供对 DynamoDB Streams 的列表和读取权限以及对 CloudWatch Logs 的写入权限。

使用此策略

您可以将 AWSLambdaDynamoDBExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:09 UTC
- 编辑时间：2015 年 4 月 9 日 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaENIManagementAccess

AWSLambdaENIManagementAccess 是一项 [AWS 托管策略](#)：为 Lambda 函数提供管理已启用 VPC 的 Lambda 函数所使用的 ENI (创建、描述、删除) 的最低权限。

使用此策略

您可以将 AWSLambdaENIManagementAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 6 日 00:37 UTC
- 编辑时间：2020 年 10 月 1 日 20:07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaExecute

AWSLambdaExecute 是一项 [AWS 托管策略](#)：提供对 S3 的 Put、Get 权限以及对 CloudWatch Logs 的完全访问权限。

使用此策略

您可以将 AWSLambdaExecute 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaExecute

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaFullAccess

AWSLambdaFullAccess 是一项 [AWS 托管策略](#)：此策略很快将被弃用。有关指南，请参阅文档：<https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html>。提供对 Lambda、S3、DynamoDB、CloudWatch Metrics 和 Logs 的完全访问权限。

使用此策略

您可以将 AWSLambdaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2017 年 11 月 27 日 23:22 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaInvocation-DynamoDB

AWSLambdaInvocation-DynamoDB 是一项 [AWS 托管策略](#)：提供对 DynamoDB Streams 的读取权限。

使用此策略

您可以将 AWSLambdaInvocation-DynamoDB 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2015 年 2 月 6 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaKinesisExecutionRole

AWSLambdaKinesisExecutionRole 是一项 [AWS 托管策略](#)：提供对 Kinesis 流的列表和读取权限以及对 CloudWatch Logs 的写入权限。

使用此策略

您可以将 AWSLambdaKinesisExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 4 月 9 日 15:14 UTC
- 编辑时间：2018 年 11 月 19 日 20:09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaMSKExecutionRole

AWSLambdaMSKExecutionRole 是一项 [AWS 托管策略](#)：提供访问 VPC 内的 MSK 集群、管理 VPC 中的 ENI (创建、描述、删除) 所需的权限，以及对 CloudWatch Logs 的写入权限。

使用此策略

您可以将 AWSLambdaMSKExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 11 日 17:35 UTC
- 编辑时间：2022 年 8 月 2 日 20:08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaReplicator

AWSLambdaReplicator 是一项 [AWS 托管策略](#)：向 Lambda Replicator 授予跨区域复制函数所需的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2017 年 5 月 23 日 17:53 UTC
- 编辑时间 : 2017 年 12 月 8 日 00:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaRole

AWSLambdaRole 是一项 [AWS 托管策略](#)：AWS Lambda 服务角色的默认策略。

使用此策略

您可以将 AWSLambdaRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaSQSQueueExecutionRole

AWSLambdaSQSQueueExecutionRole 是一项 [AWS 托管策略](#)：提供对 SQS 队列的接收消息、删除消息和读取属性的权限，以及对 CloudWatch Logs 的写入权限。

使用此策略

您可以将 AWSLambdaSQSQueueExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2018 年 6 月 14 日 21:50 UTC
- 编辑时间：2018 年 6 月 14 日 21:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs>DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLambdaVPCAccessExecutionRole

AWSLambdaVPCAccessExecutionRole 是一项 [AWS 托管策略](#)：为访问 VPC 内的资源时执行 Lambda 函数提供最低权限——创建、描述、删除网络接口和写入日志权限。CloudWatch

使用此策略

您可以将 AWSLambdaVPCAccessExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 2 月 11 日 23:15 UTC
- 编辑时间：世界标准时间 2024 年 1 月 5 日 22:38
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerConsumptionPolicy

AWSLicenseManagerConsumptionPolicy 是一项 [AWS 托管策略](#)：提供权限，以允许访问 AWS License Manager API 操作，以便使用用户拥有授权的许可证。

使用此策略

您可以将 AWSLicenseManagerConsumptionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 8 月 11 日 23:18 UTC
- 编辑时间：2021 年 8 月 11 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS License Manager Linux 订阅服务代表您管理资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2022 年 12 月 20 日 18:54 UTC
- 编辑时间 : 2022 年 12 月 20 日 18:54 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerMasterAccountRolePolicy

AWSLicenseManagerMasterAccountRolePolicy 是一项 [AWS 托管策略](#)：AWS License Manager 服务主账户角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:03 UTC
- 编辑时间：2022 年 5 月 31 日 20:50 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerMemberAccountRolePolicy

AWSLicenseManagerMemberAccountRolePolicy 是一项 [AWS 托管策略](#)：AWS License Manager 服务成员账户角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:04 UTC
- 编辑时间：2019 年 11 月 15 日 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerServiceRolePolicy

AWSLicenseManagerServiceRolePolicy 是一项 [AWS 托管策略](#) : AWS License Manager 服务默认角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 19:02 UTC
- 编辑时间：2021 年 7 月 30 日 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

AWSLicenseManagerUserSubscriptionsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS License Manager 用户订阅服务代表您管理资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 30 日 01:17 UTC
- 编辑时间：2022 年 11 月 21 日 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "bz0vcy31ooqlzk5tsash4r1lik",
        "d44g89hc0gp9jdzm99rznthpw",
        "77yzkpa7kveely1tt7wnsdwoc"
      ]
    }
  },
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSM2ServicePolicy

AWSM2ServicePolicy 是一项 [AWS 托管策略](#)：允许 AWS M2 代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 6 月 7 日 20:26 UTC
- 编辑时间：2022 年 6 月 7 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSManagedServices_ContactsServiceRolePolicy

AWSManagedServices_ContactsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Managed Services 读取 AWS 资源上标签的值

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 23 日 17:07 UTC
- 编辑时间：2023 年 3 月 23 日 17:07 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSManagedServices_ContactsServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Managed Services – 用于管理检测性控制基础设施的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 12 月 19 日 23:11 UTC
- 编辑时间：2022 年 12 月 19 日 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSManagedServices_EventsServiceRolePolicy

AWSManagedServices_EventsServiceRolePolicy 是一项 [AWS 托管策略](#)：用于启用 AMS 事件处理器功能的 AWS Managed Services 策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 2 月 7 日 18:41 UTC
- 编辑时间：2023 年 2 月 7 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSManagedServicesDeploymentToolkitPolicy

AWSManagedServicesDeploymentToolkitPolicy 是一项 [AWS 托管策略](#)：允许 AWS Managed Services 代表您管理部署工具包。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 6 月 9 日 18:33 UTC
- 编辑时间：2023 年 5 月 10 日 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceAmiIngestion

AWSMarketplaceAmiIngestion 是一项 [AWS 托管策略](#)：允许 AWS Marketplace 复制您的亚马逊机器映像 (AMI) 以便在 AWS Marketplace 上架

使用此策略

您可以将 AWSMarketplaceAmiIngestion 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 25 日 20:55 UTC
- 编辑时间：2020 年 9 月 25 日 20:55 UTC

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceDeploymentServiceRolePolicy

AWSMarketplaceDeploymentServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Marketplace 为您在 AWS Marketplace 订阅的产品创建和管理卖家部署参数。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 15 日 23:34 UTC
- 编辑时间：2023 年 11 月 15 日 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceFullAccess

AWSMarketplaceFullAccess 是一项 [AWS 托管策略](#)：提供订阅或取消订阅 AWS Marketplace 软件的功能，允许用户从 Marketplace“您的软件”页面管理 Marketplace 软件实例，并提供对 EC2 的管理访问权限。

使用此策略

您可以将 AWSMarketplaceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 11 日 17:21 UTC
- 编辑时间：2022 年 3 月 4 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceGetEntitlements

AWSMarketplaceGetEntitlements 是一项 [AWS 托管策略](#)：提供对 AWS Marketplace Entitlements 的读取权限

使用此策略

您可以将 AWSMarketplaceGetEntitlements 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 3 月 27 日 19:37 UTC
- 编辑时间：2017 年 3 月 27 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
    },
  ],
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceImageBuildFullAccess

AWSMarketplaceImageBuildFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Marketplace Private Image Build 功能的完全访问权限。除了创建私有映像外，它还提供向映像添加标签、启动和终止 EC2 实例的权限。

使用此策略

您可以将 AWSMarketplaceImageBuildFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 7 月 31 日 23:29 UTC
- 编辑时间：2022 年 3 月 4 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceLicenseManagementServiceRolePolicy

AWSMarketplaceLicenseManagementServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS Marketplace 使用或管理的 AWS 服务和资源，以进行许可证管理。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2020 年 12 月 3 日 08:33 UTC
- 编辑时间：2020 年 12 月 3 日 08:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions 是一项 [AWS 托管策略](#)：提供订阅和取消订阅 AWS Marketplace 软件的功能

使用此策略

您可以将 AWSMarketplaceManageSubscriptions 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2023 年 1 月 19 日 23:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceMeteringFullAccess

AWSMarketplaceMeteringFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Marketplace Metering 的完全访问权限。

使用此策略

您可以将 AWSMarketplaceMeteringFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2016 年 3 月 17 日 22:39 UTC
- 编辑时间：2016 年 3 月 17 日 22:39 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceMeteringRegisterUsage

AWSMarketplaceMeteringRegisterUsage 是一项 [AWS 托管策略](#)：提供通过 AWS Marketplace Metering 服务注册资源和跟踪使用情况的权限。

使用此策略

您可以将 `AWSMarketplaceMeteringRegisterUsage` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 21 日 01:17 UTC
- 编辑时间：2019 年 11 月 21 日 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceProcurementSystemAdminFullAccess

AWSMarketplaceProcurementSystemAdminFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Marketplace eProcurement 集成的所有管理操作的完全访问权限。

使用此策略

您可以将 AWSMarketplaceProcurementSystemAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 25 日 13:07 UTC
- 编辑时间：2019 年 6 月 25 日 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*"
      ]
    }
  ]
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplacePurchaseOrdersServiceRolePolicy

AWSMarketplacePurchaseOrdersServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Marketplace 服务访问采购订单管理。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 27 日 15:12 UTC
- 编辑时间：2021 年 10 月 27 日 15:12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceRead-only

AWSMarketplaceRead-only 是一项 [AWS 托管策略](#)：提供审核 AWS Marketplace 订阅的功能

使用此策略

您可以将 AWSMarketplaceRead-only 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：2023 年 1 月 19 日 23:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceResaleAuthorizationServiceRolePolicy

AWSMarketplaceResaleAuthorizationServiceRolePolicy是一项[AWS 托管策略](#)，它：允许访问转售授权 AWS 服务 以及由其使用或管理 AWS Marketplace 的资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 3 月 5 日 18:47
- 编辑时间：世界标准时间 2024 年 3 月 5 日 18:47

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

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceSellerFullAccess

AWSMarketplaceSellerFullAccess 是一项 [AWS 托管策略](#)，它：提供对卖家操作 AWS Marketplace 以及其他 AWS 服务（例如 AMI 管理）的所有操作的完全访问权限。

使用此策略

您可以将 AWSMarketplaceSellerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 2 日 20:40 UTC

- 编辑时间：世界标准时间 2024 年 3 月 15 日 16:09
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMarketplaceSellerProductsFullAccess

AWSMarketplaceSellerProductsFullAccess 是一项 [AWS 托管策略](#)：为卖家提供对 AWS Marketplace“管理产品”页面以及其他 AWS 服务（例如 AMI 管理）的完全访问权限。

使用此策略

您可以将 `AWSMarketplaceSellerProductsFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 7 月 2 日 21:06 UTC
- 编辑时间 : 2023 年 7 月 18 日 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMarketplaceSellerProductsReadOnly

AWSMarketplaceSellerProductsReadOnly 是一项 [AWS 托管策略](#)：为卖家提供对 AWS Marketplace“管理页面”页面的只读访问权限。

使用此策略

您可以将 AWSMarketplaceSellerProductsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 2 日 21:40 UTC
- 编辑时间：2022 年 11 月 19 日 00:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMediaConnectServicePolicy

AWSMediaConnectServicePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS 服务及 MediaConnect 使用或管理的资源的默认策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 3 日 22:11 UTC
- 编辑时间：2023 年 4 月 3 日 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMediaTailorServiceRolePolicy

AWSMediaTailorServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 MediaTailor 使用或管理的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 17 日 22:27 UTC
- 编辑时间：2021 年 9 月 17 日 22:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubDiscoveryAccess

AWSMigrationHubDiscoveryAccess 是一项 [AWS 托管策略](#)：此策略允许 AWSMigrationHubService 代表客户调用 AWSApplicationDiscoveryService。

使用此策略

您可以将 AWSMigrationHubDiscoveryAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:30 UTC
- 编辑时间：2020 年 8 月 6 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : [
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubDMSAccess

AWSMigrationHubDMSAccess 是一项 [AWS 托管策略](#)：此策略允许 Database Migration Service 在客户账户中担任角色以调用 Migration Hub

使用此策略

您可以将 AWSMigrationHubDMSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 14:00 UTC
- 编辑时间：2019 年 10 月 7 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubFullAccess

AWSMigrationHubFullAccess 是一项 [AWS 托管策略](#)：该托管策略为客户提供对 Migration Hub 服务的访问权限

使用此策略

您可以将 AWSMigrationHubFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 8 月 14 日 14:02 UTC
- 编辑时间：2019 年 6 月 19 日 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubOrchestratorConsoleFullAccess

AWSMigrationHubOrchestratorConsoleFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Migration Hub、AWS Application Discovery Service、Amazon Simple Storage Service 和 AWS Secrets Manager 的有限访问权限。此策略还授予对 AWS Migration Hub Orchestrator 服务的完全访问权限。

使用此策略

您可以将 AWSMigrationHubOrchestratorConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:26 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 17:34
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MH0",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MH0",
      "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*"
  }
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubOrchestratorInstanceRolePolicy

AWSMigrationHubOrchestratorInstanceRolePolicy 是一项 [AWS 托管策略](#)：需要为 SAP 和 MGN 迁移的实例附加此策略，以便我们的服务通过从 S3 下载脚本来编排实例，并在 EC2 实例中获取密钥值。

使用此策略

您可以将 AWSMigrationHubOrchestratorInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:43 UTC
- 编辑时间：2022 年 4 月 20 日 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubOrchestratorPlugin

AWSMigrationHubOrchestratorPlugin 是一项 [AWS 托管策略](#)：为 AWS Migration Hub Orchestrator 提供对 Amazon Simple Storage Service、AWS Secrets Manager 和 Plugin 相关操作的有限访问权限。

使用此策略

您可以将 `AWSMigrationHubOrchestratorPlugin` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 20 日 02:25 UTC
- 编辑时间：2022 年 4 月 20 日 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubOrchestratorServiceRolePolicy

AWSMigrationHubOrchestratorServiceRolePolicy 是一项 [AWS 托管策略](#)：为 Migration Hub Orchestrator 提供迁移与现代化您的本地工作负载所需的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 4 月 20 日 02:24 UTC
- 编辑时间：世界标准时间 2024 年 3 月 4 日 18:25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSMigrationHubRefactorSpaces- EnvironmentsWithoutBridgesFullAccess

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 是一项 [AWS 托管策略](#)：授予对 AWS Migration Hub Refactor Spaces 及其他 AWS 相关服务的完全访问权限，但使用没有网桥的环境时不需要的 AWS Transit Gateway 和 EC2 安全组除外。此策略还会排除 AWS Lambda 和 AWS Resource Access Manager 所需的权限，因为可以根据标签来缩小它们的范围。

使用此策略

您可以将 AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 4 月 3 日 20:09 UTC
- 编辑时间：2023 年 7 月 20 日 15:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 是一项 [AWS 托管策略](#)：在传递给 SSM 自动化文档 AWSRefactorSpaces-CreateResources 的 IAM 服务角色中用于授予所需权限，以运行自动化。此策略授予对 EC2 标签的读取/写入权限，以跟踪自动化进度。启用 Refactor Spaces 环境的网桥后，自动化还会将环境的安全组添加到 EC2 实例，以允许来自环境中其他 Refactor Spaces 服务的流量。此策略还授予 Application Migration Service 的启动后操作 SSM 参数的访问权限。

使用此策略

您可以将 AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 8 月 10 日 15:08 UTC
- 编辑时间：2023 年 8 月 10 日 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubRefactorSpacesFullAccess

AWSMigrationHubRefactorSpacesFullAccess 是一项 [AWS 托管策略](#)：授予对 AWS MigrationHub Refactor Spaces、AWS MigrationHub Refactor Spaces 控制台功能和其他相关 AWS 服务的完全访问权限，但 AWS Lambda 和 AWS Resource Access Manager 所需的权限除外，因为可以根据标签来缩小它们的范围。

使用此策略

您可以将 AWSMigrationHubRefactorSpacesFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 11 月 29 日 07:12 UTC
- 编辑时间：2023 年 7 月 19 日 19:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubRefactorSpacesServiceRolePolicy

AWSMigrationHubRefactorSpacesServiceRolePolicy 是一项 [AWS 托管策略](#)：提供对 AWS Migration Hub Refactor Spaces 管理或使用的 AWS 资源的访问权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 29 日 06:50 UTC
- 编辑时间：2023 年 7 月 20 日 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-
n1b-*"
  },
  {

```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubSMSAccess

AWSMigrationHubSMSAccess 是一项 [AWS 托管策略](#)：此策略允许 Server Migration Service 在客户账户中担任角色以调用 Migration Hub

使用此策略

您可以将 AWSMigrationHubSMSAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 8 月 14 日 13:57 UTC
- 编辑时间：2019 年 10 月 7 日 18:01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubStrategyCollector

AWSMigrationHubStrategyCollector 是一项 [AWS 托管策略](#)：授予允许与 AWS Migration Hub Strategy Recommendations 服务进行通信的权限、对该服务相关的 S3 桶的读取/写入权限、Amazon API Gateway 向 AWS 上传日志和指标的访问权限、AWS Secrets Manager 获取凭证的权限，以及对任何相关服务的访问权限。

使用此策略

您可以将 AWSMigrationHubStrategyCollector 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 19 日 20:15 UTC
- 编辑时间：世界标准时间 2024 年 2 月 5 日 18:57
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubStrategyConsoleFullAccess

AWSMigrationHubStrategyConsoleFullAccess 是一项 [AWS 托管策略](#)：授予对 AWS Migration Hub Strategy Recommendations 服务的完全访问权限以及通过 AWS Management Console 访问相关 AWS 服务的权限。

使用此策略

您可以将 AWSMigrationHubStrategyConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 10 月 19 日 20:13 UTC
- 编辑时间：2022 年 11 月 9 日 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMigrationHubStrategyServiceRolePolicy

AWSMigrationHubStrategyServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问由 AWS Migration Hub Strategy Recommendations 服务使用或管理的 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 19 日 20:02 UTC

- 编辑时间：2021 年 10 月 19 日 20:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMobileHub_FullAccess

AWSMobileHub_FullAccess 是一项 [AWS 托管策略](#)：此策略可以附加到任何用户、角色或组，以授予用户在 AWS Mobile Hub 中创建、删除和修改项目（及其关联的 AWS 资源）的权限。这还包括为每个 Mobile Hub 项目生成和下载示例移动应用程序源代码的权限。

使用此策略

您可以将 AWSMobileHub_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 5 日 19:56 UTC
- 编辑时间：2019 年 12 月 19 日 23:15 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_FullAccess

策略版本

策略版本：v14（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMobileHub_ReadOnly

AWSMobileHub_ReadOnly 是一项 [AWS 托管策略](#)：此策略可以附加到任何用户、角色或组，以授予用户在 AWS Mobile Hub 中列出和查看项目的权限。这还包括为每个 Mobile Hub 项目生成和下载示例移动应用程序源代码的权限。它不允许用户修改任何 Mobile Hub 项目的任何配置。

使用此策略

您可以将 AWSMobileHub_ReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间 : 2016 年 1 月 5 日 19:55 UTC
- 编辑时间 : 2018 年 7 月 23 日 21:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly

策略版本

策略版本 : v10 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSMSKReplicatorExecutionRole

AWSMSKReplicatorExecutionRole 是一项 [AWS 托管策略](#)：向 Amazon MSK Replicator 授予在 MSK 集群之间复制数据的权限。

使用此策略

您可以将 AWSMSKReplicatorExecutionRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2023 年 12 月 6 日 00:07

- 编辑时间：世界标准时间 2023 年 12 月 6 日 00:07
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSNetworkFirewallServiceRolePolicy

AWSNetworkFirewallServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWSNetworkFirewall 为您的防火墙创建和管理必要的资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 17 日 17:17 UTC
- 编辑时间：2023 年 3 月 30 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSNetworkManagerCloudWANServiceRolePolicy

AWSNetworkManagerCloudWANServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 NetworkManager 访问与您的核心网络关联的资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 12 日 12:17 UTC
- 编辑时间：2022 年 7 月 12 日 12:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2>DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ]
    }
  ],
}
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSNetworkManagerFullAccess

AWSNetworkManagerFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon NetworkManager 的完全访问权限。

使用此策略

您可以将 AWSNetworkManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 17:37 UTC
- 编辑时间：2019 年 12 月 3 日 17:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSNetworkManagerReadOnlyAccess

AWSNetworkManagerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon NetworkManager 的只读访问权限。

使用此策略

您可以将 AWSNetworkManagerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 3 日 17:35 UTC

- 编辑时间：2019 年 12 月 3 日 17:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSNetworkManagerServiceRolePolicy

AWSNetworkManagerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 NetworkManager 访问与您的全球网络关联的资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 14:03 UTC
- 编辑时间：2022 年 7 月 27 日 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorks_FullAccess

AWSOpsWorks_FullAccess 是一项 [AWS 托管策略](#)：提供对 AWS OpsWorks 的完全访问权限。

使用此策略

您可以将 AWSOpsWorks_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 1 月 22 日 16:29 UTC
- 编辑时间：2021 年 1 月 22 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksCloudWatchLogs

AWSOpsWorksCloudWatchLogs 是一项 [AWS 托管策略](#)：允许启用了 CWLogs 集成的 OpsWorks 实例发送日志并创建所需的日志组

使用此策略

您可以将 AWSOpsWorksCloudWatchLogs 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 3 月 30 日 17:47 UTC
- 编辑时间：2017 年 3 月 30 日 17:47 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksCMInstanceProfileRole

AWSOpsWorksCMInstanceProfileRole 是一项 [AWS 托管策略](#)：为 OpsWorks CM 启动的实例提供 S3 访问权限。

使用此策略

您可以将 AWSOpsWorksCMInstanceProfileRole 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2016 年 11 月 24 日 09:48 UTC
- 编辑时间：2021 年 4 月 23 日 17:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksCMServiceRole

AWSOpsWorksCMServiceRole 是一项 [AWS 托管策略](#)：用于创建 OpsWorks CM 服务器的服务角色策略。

使用此策略

您可以将 AWSOpsWorksCMServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 11 月 24 日 09:49 UTC
- 编辑时间：2021 年 4 月 23 日 17:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole

策略版本

策略版本：v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksInstanceRegistration

AWSOpsWorksInstanceRegistration 是一项 [AWS 托管策略](#)：为 Amazon EC2 实例提供向 AWS OpsWorks 堆栈注册的权限。

使用此策略

您可以将 AWSOpsWorksInstanceRegistration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 6 月 3 日 14:23 UTC
- 编辑时间：2016 年 6 月 3 日 14:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksRegisterCLI_EC2

AWSOpsWorksRegisterCLI_EC2 是一项 [AWS 托管策略](#)：允许通过 OpsWorks CLI 注册 EC2 实例的策略

使用此策略

您可以将 AWSOpsWorksRegisterCLI_EC2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 18 日 15:56 UTC

- 编辑时间 : 2019 年 6 月 18 日 15:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOpsWorksRegisterCLI_OnPremises

AWSOpsWorksRegisterCLI_OnPremises 是一项 [AWS 托管策略](#)：允许通过 OpsWorks CLI 注册本地实例的策略

使用此策略

您可以将 AWSOpsWorksRegisterCLI_OnPremises 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 18 日 15:33 UTC
- 编辑时间：2019 年 6 月 18 日 15:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOrganizationsFullAccess

AWSOrganizationsFullAccess 是一项 [AWS 托管策略](#)，它：提供对 Organizations 的完全 AWS 访问权限。

使用此策略

您可以将 AWSOrganizationsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 6 日 20:31 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 17:49
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}  
]  
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOrganizationsReadOnlyAccess

AWSOrganizationsReadOnlyAccess 是一个 [AWS 托管策略](#)，它：提供对 Organizations 的只读 AWS 访问权限。

使用此策略

您可以将 AWSOrganizationsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 6 日 20:32 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 17:36
- ARN: arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSOrganizationsServiceTrustPolicy

AWSOrganizationsServiceTrustPolicy 是一项 [AWS 托管策略](#)：此策略允许 AWS Organizations 与其他经批准的 AWS 服务 共享信任，以简化客户配置。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 10 日 23:04 UTC
- 编辑时间：2017 年 11 月 1 日 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOutpostsAuthorizeServerPolicy

AWSOutpostsAuthorizeServerPolicy 是一项 [AWS 托管策略](#)：此策略授予允许您在本地网络上安装 Outpost 服务器的权限。

使用此策略

您可以将 AWSOutpostsAuthorizeServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 1 月 4 日 19:23 UTC
- 编辑时间：2023 年 1 月 4 日 19:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSOutpostsServiceRolePolicy

AWSOutpostsServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略为服务相关角色策略，允许访问由 AWS Outposts 管理的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 9 日 22:55 UTC
- 编辑时间：2020 年 11 月 9 日 22:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaApplianceRolePolicy

AWSPanoramaApplianceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Panorama Appliance 上的 AWS IoT 软件将日志上传到 Amazon CloudWatch。

使用此策略

您可以将 AWSPanoramaApplianceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:13 UTC
- 编辑时间：2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaApplianceServiceRolePolicy

AWSPanoramaApplianceServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Panorama Appliance 将日志上传到 Amazon CloudWatch，并从为与 AWS Panorama 一起使用而创建的 Amazon S3 接入点获取对象。

使用此策略

您可以将 AWSPanoramaApplianceServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 10 月 20 日 12:14 UTC
- 编辑时间：2023 年 1 月 17 日 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaFullAccess

AWSPanoramaFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Panorama 的完全访问权限

使用此策略

您可以将 AWSPanoramaFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 1 日 13:12 UTC
- 编辑时间：2022 年 1 月 12 日 21:21 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaGreengrassGroupRolePolicy

AWSPanoramaGreengrassGroupRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Panorama Appliance 上的 AWS Lambda 函数管理 Panorama 中的资源，将日志和指标上传到 Amazon CloudWatch，以及管理为与 Panorama 一起使用而创建的桶中的对象。

使用此策略

您可以将 AWSPanoramaGreengrassGroupRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:10 UTC
- 编辑时间：2021 年 1 月 6 日 19:30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaSageMakerRolePolicy

AWSPanoramaSageMakerRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon SageMaker 管理与与 AWS Panorama 一起使用而创建的桶中的对象。

使用此策略

您可以将 AWSPanoramaSageMakerRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略

- 创建时间：2020 年 12 月 1 日 13:13 UTC
- 编辑时间：2020 年 12 月 1 日 13:13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3::*aws-panorama*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaServiceLinkedRolePolicy

AWSPanoramaServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Panorama 管理 AWS IoT、AWS Secrets Manager 和 AWS Panorama 中的资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 10 月 20 日 12:12 UTC
- 编辑时间：2021 年 10 月 20 日 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPanoramaServiceRolePolicy

AWSPanoramaServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Panorama 管理 Amazon S3、AWS IoT、AWS IoT GreenGrass、AWS Lambda、Amazon SageMaker 和 Amazon CloudWatch Logs 中的资源，并将服务角色传递给 AWS IoT、AWS IoT GreenGrass 和 Amazon SageMaker。

使用此策略

您可以将 AWSPanoramaServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 12 月 1 日 13:14 UTC
- 编辑时间：2020 年 12 月 1 日 13:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPriceListServiceFullAccess

AWSPriceListServiceFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Price List 服务的完全访问权限。

使用此策略

您可以将 AWSPriceListServiceFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 22 日 00:36 UTC
- 编辑时间：2017 年 11 月 22 日 00:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPriateCAAuditor

AWSPriateCAAuditor 是一项 [AWS 托管策略](#)：提供对 AWS Private Certificate Authority 的审计人员访问权限

使用此策略

您可以将 AWSPriateCAAuditor 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:33 UTC
- 编辑时间：2023 年 2 月 14 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriateCAAuditor

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPrivateCAFullAccess

AWSPrivateCAFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Private Certificate Authority 的完全访问权限

使用此策略

您可以将 AWSPrivateCAFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2023 年 2 月 14 日 18:20 UTC
- 编辑时间 : 2023 年 2 月 14 日 18:20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPrivateCAPrivilegedUser

AWSPrivateCAPrivilegedUser 是一项 [AWS 托管策略](#)：提供对 AWS Private Certificate Authority 的特权证书用户访问权限

使用此策略

您可以将 AWSPrivateCAPrivilegedUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:26 UTC
- 编辑时间：2023 年 2 月 14 日 18:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPivateCAReadOnly

AWSPivateCAReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS Private Certificate Authority 的只读访问权限

使用此策略

您可以将 AWSPivateCAReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:30 UTC
- 编辑时间：2023 年 2 月 14 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPivateCAReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPRivateCAUser

AWSPRivateCAUser 是一项 [AWS 托管策略](#)：提供对 AWS Private Certificate Authority 的证书用户访问权限

使用此策略

您可以将 AWSPRivateCAUser 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 2 月 14 日 18:16 UTC
- 编辑时间：2023 年 2 月 14 日 18:16 UTC
- ARN: arn:aws:iam::aws:policy/AWSPRivateCAUser

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccess是一项[AWS 托管策略](#)，它：提供对 AWS 私有市场 (Private Marketplace) 所有管理操作的完全访问权限。

使用此策略

您可以将 AWSPrivateMarketplaceAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 16:32 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:05
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSPrivateMarketplaceRequests

AWSPrivateMarketplaceRequests 是一项 [AWS 托管策略](#)：提供在 AWS Private Marketplace 中创建请求的访问权限。

使用此策略

您可以将 AWSPrivateMarketplaceRequests 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 28 日 21:44 UTC

- 编辑时间：2019 年 10 月 28 日 21:44 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPrivateNetworksServiceRolePolicy

AWSPrivateNetworksServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Private Networks 服务代表客户管理资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 12 月 16 日 23:17 UTC
- 编辑时间：2021 年 12 月 16 日 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonCodeBuildProvisioningBasicAccess

AWSProtonCodeBuildProvisioningBasicAccess 是一项 [AWS 托管策略](#)：CodeBuild 为 AWS Proton CodeBuild Provisioning 运行构建所需的权限。

使用此策略

您可以将 AWSProtonCodeBuildProvisioningBasicAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 9 日 21:04 UTC
- 编辑时间：2022 年 11 月 9 日 21:04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonCodeBuildProvisioningServiceRolePolicy

AWSProtonCodeBuildProvisioningServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Proton 代表您使用 CodeBuild 和其他 AWS 服务管理 Proton 资源配置。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 9 日 21:32 UTC
- 编辑时间：2023 年 5 月 17 日 16:11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonDeveloperAccess

AWSProtonDeveloperAccess 是一项 [AWS 托管策略](#)：提供对 AWS Proton API 和 Management Console 的访问权限，但不允许管理 Proton 模板或环境。

使用此策略

您可以将 AWSProtonDeveloperAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:02 UTC
- 编辑时间：2022 年 11 月 18 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]

```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonFullAccess

AWSProtonFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Proton API 和 Management Console 的完全访问权限。除了这些权限外，还需要访问 Amazon S3 才能从 S3 桶注册模板包，以及访问 Amazon IAM 以创建和管理 Proton 的服务角色。

使用此策略

您可以将 AWSProtonFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:07 UTC
- 编辑时间：2022 年 6 月 20 日 12:36 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonReadOnlyAccess

AWSProtonReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Proton API 和 Management Console 的只读访问权限。

使用此策略

您可以将 AWSProtonReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 2 月 17 日 19:09 UTC
- 编辑时间：2022 年 11 月 18 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonServiceGitSyncServiceRolePolicy

AWSProtonServiceGitSyncServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Proton 将您的服务、环境和组件定义从 Git 存储库同步到 AWS Proton。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 4 日 15:55 UTC
- 编辑时间：2023 年 4 月 4 日 15:55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSProtonSyncServiceRolePolicy

AWSProtonSyncServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Proton 将您的 Git 存储库内容同步到 Proton 或将 Proton 内容同步到您的 Git 存储库。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 23 日 21:14 UTC
- 编辑时间：2021 年 11 月 23 日 21:14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSPurchaseOrdersServiceRolePolicy

AWSPurchaseOrdersServiceRolePolicy 是一项 [AWS 托管策略](#)：授予在账单控制台上查看和修改采购订单的权限

使用此策略

您可以将 AWSPurchaseOrdersServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 6 日 18:15 UTC
- 编辑时间：2023 年 7 月 17 日 18:59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuicksightAthenaAccess

AWSQuicksightAthenaAccess 是一项 [AWS 托管策略](#)：对用于 Athena 查询结果的 Athena API 和 S3 桶的 Quicksight 访问权限

使用此策略

您可以将 AWSQuicksightAthenaAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 12 月 9 日 02:31 UTC
- 编辑时间：2021 年 7 月 7 日 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

策略版本

策略版本：v10（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightDescribeRDS

AWSQuickSightDescribeRDS 是一项 [AWS 托管策略](#)：允许 QuickSight 描述 RDS 资源

使用此策略

您可以将 AWSQuickSightDescribeRDS 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:24 UTC
- 编辑时间：2015 年 11 月 10 日 23:24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightDescribeRedshift

AWSQuickSightDescribeRedshift 是一项 [AWS 托管策略](#)：允许 QuickSight 描述 Redshift 资源

使用此策略

您可以将 AWSQuickSightDescribeRedshift 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:25 UTC
- 编辑时间：2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightElasticsearchPolicy

AWSQuickSightElasticsearchPolicy 是一项 [AWS 托管策略](#)：提供访问来自 Amazon QuickSight 的 Amazon Elasticsearch 资源的权限

使用此策略

您可以将 AWSQuickSightElasticsearchPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 9 日 17:27 UTC
- 编辑时间：2021 年 9 月 7 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightIoTAnalyticsAccess

AWSQuickSightIoTAnalyticsAccess 是一项 [AWS 托管策略](#)：授予 QuickSight 对 IoT Analytics 数据集的只读访问权限

使用此策略

您可以将 `AWSQuickSightIoTAnalyticsAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 29 日 17:00 UTC
- 编辑时间 : 2017 年 11 月 29 日 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightListIAM

AWSQuickSightListIAM 是一项 [AWS 托管策略](#)：允许 QuickSight 列出 IAM 实体

使用此策略

您可以将 AWSQuickSightListIAM 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 11 月 10 日 23:25 UTC
- 编辑时间：2015 年 11 月 10 日 23:25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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



```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuicksightOpenSearchPolicy

AWSQuicksightOpenSearchPolicy 是一项 [AWS 托管策略](#)：提供访问来自 Amazon QuickSight 的 Amazon OpenSearch 资源的权限

使用此策略

您可以将 AWSQuicksightOpenSearchPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2021 年 9 月 7 日 23:26 UTC
- 编辑时间：2021 年 9 月 7 日 23:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightSageMakerPolicy

AWSQuickSightSageMakerPolicy 是一项 [AWS 托管策略](#)：提供访问来自 Amazon QuickSight 的 Amazon SageMaker 资源的权限

使用此策略

您可以将 AWSQuickSightSageMakerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 1 月 17 日 17:18 UTC
- 编辑时间：2023 年 10 月 30 日 17:57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSQuickSightTimestreamPolicy

AWSQuickSightTimestreamPolicy 是一项 [AWS 托管策略](#)：AWS Timestream API 的 AWS QuickSight 访问权限。客户可以将此策略附加到 AWS QuickSight 角色以允许检索数据和元数据。

使用此策略

您可以将 AWSQuickSightTimestreamPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 9 月 30 日 21:47 UTC
- 编辑时间：2020 年 9 月 30 日 21:47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSReachabilityAnalyzerServiceRolePolicy

AWSReachabilityAnalyzerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 VPC Reachability Analyzer 代表您访问 AWS 资源并与 AWS Organizations 集成。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 23 日 17:12 UTC
- 编辑时间：2023 年 6 月 23 日 21:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRefactoringToolkitFullAccess

AWSRefactoringToolkitFullAccess 是一项 [AWS 托管策略](#)：该策略授予通过 Microsoft Visual Studio 的 AWS Toolkit for .NET Refactoring 扩展程序使用 AWS 服务的权限。它旨在附加到本地 AWS 配置文件中。该策略允许上传应用程序构件并从 Amazon S3 下载生成的构件。它允许使用亚马逊弹性容器注册表 (Amazon ECR) Container Registry (Amazon ECR) 中存储 AWS CodeBuild 和检索映像将应用程序构建到容器映像中。它还允许将应用程序部署到 AWS 上的容器服务，例如 Amazon Elastic Container Service (Amazon ECS)、可选创建 VPC 资源、可选连接到 AWS Directory Service 等现有基础设施以及其他相关服务。

使用此策略

您可以将 AWSRefactoringToolkitFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 10 月 25 日 16:41 UTC

- 编辑时间：世界标准时间 2023 年 11 月 18 日 00:37
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRefactoringToolkitSidecarPolicy

AWSRefactoringToolkitSidecarPolicy 是一项 [AWS 托管策略](#)：此策略旨在由为使用 Microsoft Visual Studio 的 AWS Toolkit for .NET Refactoring 扩展程序在 AWS 中测试应用程序而创建的 Amazon ECS 任务使用。该策略授予从 Amazon S3 下载应用程序构件、使用 AWS Systems Manager 传达任务状态的权限以及其他所需服务的访问权限。

使用此策略

您可以将 `AWSRefactoringToolkitSidecarPolicy` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 10 月 25 日 16:41 UTC
- 编辑时间 : 2022 年 10 月 29 日 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSrePostPrivateCloudWatchAccess

AWSrePostPrivateCloudWatchAccess 是一项 [AWS 托管策略](#)，它提供 re: Post 私密访问权限以发布指标数据 CloudWatch

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 15 日 16:37 UTC

- 编辑时间：2023 年 11 月 15 日 16:37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRepostSpaceSupportOperationsPolicy

AWSRepostSpaceSupportOperationsPolicy 是一项 [AWS 托管策略](#)：此策略允许 re: Post Space 服务创建、管理和解决通过 Space 应用程序创建的支持案例。

使用此策略

您可以将 AWSRepostSpaceSupportOperationsPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 21:52
- 编辑时间：世界标准时间 2023 年 11 月 26 日 21:52
- ARN: arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ]
    }
  ]
}
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResilienceHubAssessmentExecutionPolicy

AWSResilienceHubAssessmentExecutionPolicy 是一项 [AWS 托管策略](#)：AWS Resilience Hub 服务角色允许访问其他 AWS 服务以执行评估的策略。

使用此策略

您可以将 AWSResilienceHubAssessmentExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 6 月 27 日 12:32 UTC
- 编辑时间：2023 年 10 月 29 日 16:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAssessmentExecutionPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceAccessManagerFullAccess

AWSResourceAccessManagerFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Resource Access Manager 的完全访问权限

使用此策略

您可以将 AWSResourceAccessManagerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 4 日 17:28 UTC
- 编辑时间：2019 年 6 月 4 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceAccessManagerReadOnlyAccess

AWSResourceAccessManagerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Resource Access Manager 的只读访问权限。

使用此策略

您可以将 AWSResourceAccessManagerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 9 日 20:58 UTC
- 编辑时间：2019 年 12 月 9 日 20:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceAccessManagerResourceShareParticipantAccess

AWSResourceAccessManagerResourceShareParticipantAccess 是一项 [AWS 托管策略](#)：提供资源共享参与者所需的 AWS Resource Access Manager API 的访问权限。

使用此策略

您可以将 AWSResourceAccessManagerResourceShareParticipantAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 9 日 20:41 UTC
- 编辑时间：2019 年 12 月 9 日 20:41 UTC
- ARN: arn:aws:iam::aws:policy/
AWSResourceAccessManagerResourceShareParticipantAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceAccessManagerServiceRolePolicy

AWSResourceAccessManagerServiceRolePolicy 是一项 [AWS 托管策略](#)：包含对客户组织结构的只读 AWS Resource Access Manager 访问权限的策略。它还包含自行删除角色的 IAM 权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 14 日 19:28 UTC
- 编辑时间：2018 年 11 月 14 日 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceExplorerFullAccess

AWSResourceExplorerFullAccess 是一项 [AWS 托管策略](#)：此策略授予访问资源管理器资源的管理权限，并向其他 AWS 服务授予只读权限以支持此访问权限。

使用此策略

您可以将 AWSResourceExplorerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 7 日 20:01 UTC
- 编辑时间：2023 年 11 月 14 日 16:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceExplorerOrganizationsAccess

AWSResourceExplorerOrganizationsAccess 是一项 [AWS 托管策略](#)：此策略授予资源管理器管理权限，并向其他 AWS 服务授予只读权限以支持此访问权限。AWS Organizations 管理员需要获得这些权限才能在控制台中设置和管理多账户搜索。

使用此策略

您可以将 AWSResourceExplorerOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 11 月 14 日 17:01 UTC
- 编辑时间：2023 年 11 月 14 日 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceExplorerReadOnlyAccess

AWSResourceExplorerReadOnlyAccess 是一项 [AWS 托管策略](#)：此策略授予搜索和查看资源管理器资源的只读权限，并向其他 AWS 服务授予只读权限以支持此访问权限。

使用此策略

您可以将 AWSResourceExplorerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 7 日 19:56 UTC

- 编辑时间：2023 年 11 月 14 日 16:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceExplorerServiceRolePolicy

AWSResourceExplorerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许资源浏览器代表您查看资源和 CloudTrail 事件，从而为您的资源编制索引以供搜索。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 10 月 25 日 20:35 UTC
- 编辑时间：世界标准时间 2023 年 12 月 20 日 13:58
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"resiliencyhub:ListApps",
"resiliencyhub: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" : [
    "*"
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSResourceGroupsReadOnlyAccess

AWSResourceGroupsReadOnlyAccess 是一项 [AWS 托管策略](#)：这是 AWS Resource Groups 的只读策略

使用此策略

您可以将 `AWSResourceGroupsReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 3 月 7 日 10:27 UTC
- 编辑时间 : 2019 年 2 月 5 日 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRoboMaker_FullAccess

AWSRoboMaker_FullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 AWS RoboMaker 的完全访问权限。还提供对相关服务（例如 S3、IAM）的部分访问权限。

使用此策略

您可以将 AWSRoboMaker_FullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 10 日 18:34 UTC
- 编辑时间：2021 年 9 月 16 日 21:06 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

策略版本

策略版本：v2（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRoboMakerReadOnlyAccess

AWSRoboMakerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 和 SDK 访问 AWS RoboMaker 的只读访问权限

使用此策略

您可以将 AWSRoboMakerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 26 日 05:30 UTC
- 编辑时间：2020 年 8 月 28 日 23:10 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRoboMakerServicePolicy

AWSRoboMakerServicePolicy 是一项 [AWS 托管策略](#)：RoboMaker 服务策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 06:30 UTC
- 编辑时间：2021 年 11 月 11 日 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRoboMakerServiceRolePolicy

AWSRoboMakerServiceRolePolicy 是一项 [AWS 托管策略](#) : RoboMaker 服务策略

使用此策略

您可以将 AWSRoboMakerServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 11 月 26 日 05:33 UTC
- 编辑时间 : 2018 年 11 月 26 日 05:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSRolesAnywhereServicePolicy

AWSRolesAnywhereServicePolicy 是一项 [AWS 托管策略](#)：允许 IAM Roles Anywhere 向 CloudWatch 发布服务/使用情况指标，并代表您检查私有证书颁发机构的状况。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 7 月 5 日 15:26 UTC
- 编辑时间：2022 年 7 月 5 日 15:26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSS3OnOutpostsServiceRolePolicy

AWSS3OnOutpostsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Outposts 服务上的 Amazon S3 代表您管理 EC2 网络资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 10 月 3 日 20:32 UTC
- 编辑时间：2023 年 10 月 3 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSavingsPlansFullAccess

AWSSavingsPlansFullAccess 是一项 [AWS 托管策略](#)：提供对 Savings Plans 服务的完全访问权限

使用此策略

您可以将 AWSSavingsPlansFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 6 日 22:45 UTC
- 编辑时间：2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSavingsPlansReadOnlyAccess

AWSSavingsPlansReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对节省计划服务的只读访问权限

使用此策略

您可以将 AWSSavingsPlansReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 6 日 22:45 UTC
- 编辑时间：2019 年 11 月 6 日 22:45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSecurityHubFullAccess

AWSSecurityHubFullAccess 是一项 [AWS 托管策略](#)：提供对使用 AWS Security Hub 的完全访问权限。

使用此策略

您可以将 AWSSecurityHubFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 23:54 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 21:10

- ARN: arn:aws:iam::aws:policy/AWSSecurityHubFullAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSecurityHubOrganizationsAccess

AWSecurityHubOrganizationsAccess 是一项 [AWS 托管策略](#)：授予在组织内启用和管理 AWS Security Hub 的权限。包括在整个组织中启用该服务，以及确定该服务的委托管理员账户。

使用此策略

您可以将 AWSecurityHubOrganizationsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2021 年 3 月 15 日 20:53 UTC
- 编辑时间：世界标准时间 2023 年 11 月 16 日 21:13
- ARN: `arn:aws:iam::aws:policy/AWSecurityHubOrganizationsAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSecurityHubReadOnlyAccess

AWSecurityHubReadOnlyAccess是一项[AWS 托管策略](#)，它：提供对 Sec AWS urity Hub 资源的只读访问权限

使用此策略

您可以将 AWSecurityHubReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 28 日 01:34 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 23:45
- ARN: arn:aws:iam::aws:policy/AWSecurityHubReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

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

```
{
  "Sid" : "AWSSecurityHubReadOnlyAccess",
  "Effect" : "Allow",
  "Action" : [
    "securityhub:Get*",
    "securityhub:List*",
    "securityhub:BatchGet*",
    "securityhub:Describe*"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSSecurityHubServiceRolePolicy

AWSSecurityHubServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Security Hub 访问您的资源所需的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 27 日 23:47 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 03:46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy

策略版本

策略版本 : v14 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}

```

```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogAdminFullAccess

AWSServiceCatalogAdminFullAccess 是一项 [AWS 托管策略](#)：提供对服务目录管理功能的完全访问权限

使用此策略

您可以将 AWSServiceCatalogAdminFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 15 日 17:19 UTC
- 编辑时间：2023 年 4 月 13 日 18:43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogAdminReadOnlyAccess

AWSServiceCatalogAdminReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对服务目录管理功能的只读访问权限

使用此策略

您可以将 AWSServiceCatalogAdminReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 10 月 25 日 18:53 UTC
- 编辑时间 : 2019 年 10 月 25 日 18:53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogAppRegistryFullAccess

AWSServiceCatalogAppRegistryFullAccess 是一项 [AWS 托管策略](#)：提供对服务目录 App Registry 功能的完全访问权限

使用此策略

您可以将 `AWSServiceCatalogAppRegistryFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 12 日 22:25 UTC
- 编辑时间：世界标准时间 2023 年 12 月 7 日 21:50
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*:*:*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogAppRegistryReadOnlyAccess

AWSServiceCatalogAppRegistryReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对服务目录 App Registry 功能的只读访问权限

使用此策略

您可以将 `AWSServiceCatalogAppRegistryReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 11 月 12 日 22:34 UTC
- 编辑时间 : 2022 年 11 月 17 日 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogAppRegistryServiceRolePolicy

AWSServiceCatalogAppRegistryServiceRolePolicy 是一项 [AWS 托管策略](#)：允许服务目录 AppRegistry 代表您管理资源组

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 5 月 18 日 22:18 UTC
- 编辑时间：2022 年 10 月 26 日 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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*"
    ]
  }
]
```

```
    ]  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogEndUserFullAccess

AWSServiceCatalogEndUserFullAccess 是一项 [AWS 托管策略](#)：提供对服务目录最终用户功能的完全访问权限

使用此策略

您可以将 AWSServiceCatalogEndUserFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 2 月 15 日 17:22 UTC
- 编辑时间：2019 年 7 月 10 日 20:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
    }
  }
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogEndUserReadOnlyAccess

AWSServiceCatalogEndUserReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对服务目录最终用户功能的只读访问权限

使用此策略

您可以将 AWSServiceCatalogEndUserReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 10 月 25 日 18:49 UTC
- 编辑时间：2019 年 10 月 25 日 18:49 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

AWSServiceCatalogOrgsDataSyncServiceRolePolicy 是一项 [AWS 托管策略](#) : AWS ServiceCatalog 与 AWS Organizations 组织结构同步的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型 : 服务相关角色策略
- 创建时间 : 2023 年 4 月 10 日 20:48 UTC
- 编辑时间 : 2023 年 4 月 10 日 20:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceCatalogSyncServiceRolePolicy

AWSServiceCatalogSyncServiceRolePolicy 是一项 [AWS 托管策略](#) : AWS ServiceCatalog 同步来自源存储库的预置构件的服务相关角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 15 日 21:20 UTC
- 编辑时间：2022 年 11 月 15 日 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForAmazonEKSNodegroup

AWSServiceRoleForAmazonEKSNodegroup 是一项 [AWS 托管策略](#)：管理客户账户中的节点组所需的权限。这些策略与以下资源的管理有关：AutoscalingGroups SecurityGroups、LaunchTemplates 和 InstanceProfiles。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 7 日 01:34 UTC
- 编辑时间：世界标准时间 2024 年 1 月 4 日 20:37
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  }
}
```

```
    ]
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 是一项 [AWS 托管策略](#)：提供对 CloudWatch 警报所使用的 Systems Manager 资源的访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 10 月 1 日 09:49 UTC
- 编辑时间：2020 年 10 月 1 日 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 CloudWatch 代表您访问 RDS Performance Insights 指标

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 9 月 7 日 09:32 UTC
- 编辑时间：2023 年 9 月 7 日 09:32 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForCodeGuru-Profiler

AWSServiceRoleForCodeGuru-Profiler 是一项 [AWS 托管策略](#)：Amazon CodeGuru Profiler 代表您发送通知所需的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 26 日 22:04 UTC
- 编辑时间：2020 年 6 月 26 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuruProfiler

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForCodeWhispererPolicy

AWSServiceRoleForCodeWhispererPolicy 是一项 [AWS 托管策略](#)：此角色授予访问您账户中数据 CodeWhisperer 以计算账单的权限，提供在 Amazon 中创建和访问安全报告的权限 CodeGuru，以及向 CloudWatch 发送数据的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 24 日 19:39 UTC
- 编辑时间：世界标准时间 2024 年 3 月 1 日 23:35
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForEC2ScheduledInstances

AWSServiceRoleForEC2ScheduledInstances 是一项 [AWS 托管策略](#)：允许 EC2 计划实例启动和管理竞价型实例。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 10 月 12 日 18:31 UTC
- 编辑时间：2017 年 10 月 12 日 18:31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 是一项 [AWS 托管策略](#)：AWS GroundStation 使用此服务相关角色调用 EC2 来查找公有 IPv4 地址

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 12 月 13 日 23:52 UTC
- 编辑时间：2022 年 12 月 13 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
    "Action" : [
      "ec2:DescribeAddresses",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForImageBuilder

AWSServiceRoleForImageBuilder 是一项 [AWS 托管策略](#)：允许 EC2ImageBuilder 代表您调用 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 29 日 22:02 UTC
- 编辑时间：2023 年 10 月 19 日 21:30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder

策略版本

策略版本：v19 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForIoTSiteWise

AWSServiceRoleForIoTSiteWise是一项[AWS托管策略](#)：允许 AWS IoT SiteWise 配置和管理网关以及查询数据。该策略包括部署到组所需的 AWS Greengrass 权限、用于创建和更新前缀为“service”的函数的 AWS Lambda 权限，以及用于从数据存储中查询数据的 AWS IoT Analytics 权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 14 日 19:19 UTC
- 编辑时间：2023 年 11 月 13 日 18:27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForLogDeliveryPolicy

AWSServiceRoleForLogDeliveryPolicy 是一项 [AWS 托管策略](#)：允许日志传输服务通过代表您调用日志目标来传输日志。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 4 日 17:31 UTC
- 编辑时间：2021 年 7 月 15 日 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/LogDeliveryEnabled": "true"
        }
      }
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForMonitronPolicy

AWSServiceRoleForMonitronPolicy 是一项 [AWS 托管策略](#)：授予 Amazon Monitron 管理 AWS 资源的权限，包括代表您分配 AWS SSO 用户。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 2 日 19:06 UTC
- 编辑时间：2022 年 9 月 29 日 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForNeptuneGraphPolicy

AWSServiceRoleForNeptuneGraphPolicy 是一项 [AWS 托管策略](#)：提供 Cloudwatch 访问权限，用于发布 Amazon Neptune 的运行和使用指标以及日志

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 14:03
- 编辑时间：世界标准时间 2023 年 11 月 29 日 14:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRoleForPrivateMarketplaceAdminPolicy

AWSServiceRoleForPrivateMarketplaceAdminPolicy 是一项 [AWS 托管策略](#)，它：提供描述和更新 Private Marketplace 资源以及描述 AWS Organizations 的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2024 年 2 月 14 日 22:28
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:28

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSServiceRoleForSMS

AWSServiceRoleForSMS 是一项 [AWS 托管策略](#)：提供对迁移服务实例至 AWS（包括 EC2、S3 和 CloudFormation）所需的 AWS 服务和资源的访问权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 6 日 18:39 UTC
- 编辑时间：2020 年 10 月 15 日 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

策略版本

策略版本：v10（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRolePolicyForBackupReports

AWSServiceRolePolicyForBackupReports 是一项 [AWS 托管策略](#)：提供 AWS Backup 权限，以代表您创建合规性报告

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 19 日 21:16 UTC
- 编辑时间：2023 年 3 月 10 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSServiceRolePolicyForBackupRestoreTesting

AWSServiceRolePolicyForBackupRestoreTesting 是一项 [AWS 托管策略](#)：此策略包含还原测试以及清理测试期间创建的资源的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 10 日 23:37 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 22:42
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSShieldDRTAccessPolicy

AWSShieldDRTAccessPolicy 是一项 [AWS 托管策略](#)：在高严重性事件期间，为 AWS DDoS 响应团队提供您的 AWS 账户 的有限访问权限，以协助缓解 DDoS 攻击。

使用此策略

您可以将 AWSShieldDRTAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 6 月 5 日 22:29 UTC
- 编辑时间：2020 年 12 月 15 日 17:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSShieldServiceRolePolicy

AWSShieldServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Shield 代表您访问 AWS 资源以提供 DDoS 保护。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 11 月 17 日 19:17 UTC
- 编辑时间：2021 年 11 月 17 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSMForSAPServiceLinkedRolePolicy

AWSSSMForSAPServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：为 AWS Systems Manager for SAP 提供通过 AWS 管理和集成 SAP 软件所需的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 16 日 01:18 UTC
- 编辑时间：世界标准时间 2023 年 11 月 21 日 03:35
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSMOpsInsightsServiceRolePolicy

AWSSSMOpsInsightsServiceRolePolicy 是一项 [AWS 托管策略](#) :
AWSServiceRoleForAmazonSSM_OpsInsights 服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 6 月 16 日 20:12 UTC
- 编辑时间：2021 年 6 月 16 日 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSM0psInsightsServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSODirectoryAdministrator

AWSSSODirectoryAdministrator 是一项 [AWS 托管策略](#)：SSO 目录的管理员访问权限

使用此策略

您可以将 AWSSSODirectoryAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 31 日 23:54 UTC
- 编辑时间：2022 年 10 月 20 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSODirectoryReadOnly

AWSSSODirectoryReadOnly 是一项 [AWS 托管策略](#)：SSO 目录的只读访问权限

使用此策略

您可以将 AWSSSODirectoryReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 10 月 31 日 23:49 UTC

- 编辑时间：2022 年 11 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministrator 是一项 [AWS 托管策略](#)：在 AWS SSO 中提供访问权限以管理 AWS Organizations 主账户和成员账户以及云应用程序

使用此策略

您可以将 AWSSSOMasterAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:36 UTC
- 编辑时间：2022 年 10 月 20 日 20:34 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSS0CreateSLR",
      "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSOMemberAccountAdministrator

AWSSSOMemberAccountAdministrator 是一项 [AWS 托管策略](#)：在 AWS SSO 中提供访问权限以管理 AWS Organizations 成员账户以及云应用程序

使用此策略

您可以将 AWSSSOMemberAccountAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:45 UTC
- 编辑时间：2022 年 10 月 20 日 20:32 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSOReadOnly

AWSSSOReadOnly 是一项 [AWS 托管策略](#)：提供对 AWS SSO 配置的只读访问权限。

使用此策略

您可以将 AWSSSOReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 6 月 27 日 20:24 UTC
- 编辑时间：2022 年 8 月 22 日 17:23 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSSOServiceRolePolicy

AWSSSOServiceRolePolicy 是一项 [AWS 托管策略](#)：授予 AWS SSO 代表您管理 AWS 资源的权限，包括 IAM 角色、策略和 SAML IdP。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 12 月 5 日 18:36 UTC
- 编辑时间：2022 年 10 月 20 日 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

策略版本

策略版本：v17 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
    ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSStepFunctionsConsoleFullAccess

AWSStepFunctionsConsoleFullAccess 是一项 [AWS 托管策略](#)：一种用于向用户/角色等提供对 AWS StepFunctions 控制台的访问权限的访问策略。要获得完整的控制台体验，除了此策略外，用户可能还需要对可由该服务担任的其他 IAM 角色的 iam:PassRole 权限。

使用此策略

您可以将 AWSStepFunctionsConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:54 UTC
- 编辑时间：2017 年 1 月 12 日 00:19 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSStepFunctionsFullAccess

AWSStepFunctionsFullAccess 是一项 [AWS 托管策略](#)：一种用于向用户/角色等提供对 AWS StepFunctions API 的访问权限的访问策略。要获得完全访问权限，除了此策略外，用户须获得对可由该服务担任的至少一个 IAM 角色的 iam:PassRole 权限。

使用此策略

您可以将 AWSStepFunctionsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:51 UTC
- 编辑时间：2017 年 1 月 11 日 21:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSStepFunctionsReadOnlyAccess

AWSStepFunctionsReadOnlyAccess 是一项 [AWS 托管策略](#)：一种用于向用户/角色等提供对 AWS StepFunctions 服务的只读访问权限的访问策略。

使用此策略

您可以将 AWSStepFunctionsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 1 月 11 日 21:46 UTC
- 编辑时间：2017 年 11 月 10 日 22:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSStorageGatewayFullAccess

AWSStorageGatewayFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Storage Gateway 的完全访问权限。

使用此策略

您可以将 AWSStorageGatewayFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2022 年 9 月 6 日 20:26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSStorageGatewayReadOnlyAccess

AWSStorageGatewayReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Storage Gateway 的权限。

使用此策略

您可以将 AWSStorageGatewayReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2022 年 9 月 6 日 20:24 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSStorageGatewayServiceRolePolicy

AWSStorageGatewayServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Storage Gateway 用于实现其他 AWS 服务与 Storage Gateway 集成的服务相关角色。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 2 月 17 日 19:03 UTC
- 编辑时间：2021 年 2 月 17 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess 是一种 [AWS 托管策略](#)，它：

AWSSupplyChainFederationAdminAccess 为 AWS 供应链联合用户提供对 AWS 供应链应用程序的访问权限，包括在 AWS 供应链应用程序中执行操作所需的权限。该策略提供对 IAM Identity Center 用户和组的管理权限，并附加到 AWS Supply Chain 代表您创建的角色。您不应将 AWSSupplyChainFederationAdminAccess 策略附加到任何其他 IAM 实体。

使用此策略

您可以将 AWSSupplyChainFederationAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 3 月 1 日 18:54 UTC
- 编辑时间：2023 年 11 月 1 日 18:50 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportAccess

AWSSupportAccess 是一项 [AWS 托管策略](#)：允许用户访问 AWS Support Center。

使用此策略

您可以将 AWSSupportAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:41 UTC
- 编辑时间 : 2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportAppFullAccess

AWSSupportAppFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Support 应用程序和其他必需服务（例如 AWS Support 和 Service Quotas）的完全访问权限。此策略包括使用支持服务的权限，以便用户可以联系 AWS Support 以获取支持案例、更改服务限额以及创建相关的服务相关角色。

使用此策略

您可以将 AWSSupportAppFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 22 日 16:53 UTC
- 编辑时间：2022 年 8 月 22 日 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

策略版本

策略版本：v1（默认）

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Support 应用程序的只读访问权限。

使用此策略

您可以将 AWSSupportAppReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2022 年 8 月 22 日 17:01 UTC
- 编辑时间 : 2022 年 8 月 22 日 17:01 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportPlansFullAccess

AWSSupportPlansFullAccess 是一项 [AWS 托管策略](#)：提供对 supportplans 的完全访问权限。

使用此策略

您可以将 AWSSupportPlansFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 27 日 18:19 UTC
- 编辑时间：2023 年 5 月 9 日 21:07 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportPlansReadOnlyAccess

AWSSupportPlansReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 supportplans 的只读访问权限。

使用此策略

您可以将 AWSSupportPlansReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 9 月 27 日 18:08 UTC
- 编辑时间：2022 年 9 月 27 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSupportServiceRolePolicy

AWSSupportServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Support 访问 AWS 资源以提供计费、管理和支持服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 4 月 19 日 18:04 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 22:28
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

策略版本

策略版本：v34 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"d1m:getLifecyclePolicies",
"d1m: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",
"dms:describeJobLogItems",
"dms:describeJobs",
"dms:describeLaunchConfigurationTemplates",
"dms:describeRecoveryInstances",
"dms:describeRecoverySnapshots",
"dms:describeReplicationConfigurationTemplates",
"dms:describeSourceNetworks",
"dms:describeSourceServers",
"dms:getLaunchConfiguration",
"dms:getReplicationConfiguration",
"dms:listExtensibleSourceServers",
"dms:listLaunchActions",
"dms: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"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSystemsManagerAccountDiscoveryServicePolicy

AWSSystemsManagerAccountDiscoveryServicePolicy 是一项 [AWS 托管策略](#)：授予 AWS Systems Manager (SSM) 发现 AWS 账户 信息的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 10 月 24 日 17:21 UTC
- 编辑时间：2022 年 10 月 17 日 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSystemsManagerChangeManagementServicePolicy

AWSSystemsManagerChangeManagementServicePolicy 是一项 [AWS 托管策略](#)：提供对由 AWS Systems Manager 变更管理框架管理或使用的 AWS 资源的访问权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 7 日 22:21 UTC
- 编辑时间：2020 年 12 月 7 日 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSystemsManagerForSAPFullAccess

AWSSystemsManagerForSAPFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Systems Manager for SAP 服务的完全访问权限

使用此策略

您可以将 AWSSystemsManagerForSAPFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 17 日 02:11 UTC

- 编辑时间：2022 年 11 月 18 日 21:58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSystemsManagerForSAPReadOnlyAccess

AWSSystemsManagerForSAPReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Systems Manager for SAP 服务的只读访问权限

使用此策略

您可以将 AWSSystemsManagerForSAPReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 17 日 02:11 UTC
- 编辑时间：2022 年 11 月 17 日 02:11 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "ssm-sap:get*",
      "ssm-sap:list*"
    ],
    "Resource" : "arn:*:ssm-sap:*:*:*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSSystemsManagerOpsDataSyncServiceRolePolicy

AWSSystemsManagerOpsDataSyncServiceRolePolicy 是一项 [AWS 托管策略](#)：SSM Explorer 用于管理 OpsData 相关操作的 IAM 角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 4 月 26 日 20:42 UTC
- 编辑时间：2023 年 6 月 28 日 22:53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxAssetServerPolicy

AWSThinkboxAssetServerPolicy 是一项 [AWS 托管策略](#)：此策略向 AWS 门户资产服务器授予正常操作所需的必要权限。

使用此策略

您可以将 AWSThinkboxAssetServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 5 月 27 日 19:18 UTC
- 编辑时间 : 2020 年 5 月 27 日 19:18 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxAWSPortalAdminPolicy

AWSThinkboxAWSPortalAdminPolicy 是一项 [AWS 托管策略：该政策](#) 授予 AWS Thinkbox 的 Deadline 软件根据 AWS 门户管理所需的对多项 AWS 服务的完全访问权限。这包括对多种 EC2 资源类型创建任意标签的权限。

使用此策略

您可以将 AWSThinkboxAWSPortalAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:41 UTC
- 编辑时间：世界标准时间 2024 年 2 月 23 日 22:25
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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*"
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSThinkboxAWSPortalGatewayPolicy

AWSThinkboxAWSPortalGatewayPolicy 是一项 [AWS 托管策略](#)：此策略向 AWS 门户网关计算机授予正常操作所需的必要权限。

使用此策略

您可以将 AWSThinkboxAWSPortalGatewayPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 5 月 27 日 19:05 UTC
- 编辑时间 : 2020 年 6 月 30 日 16:02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:rds-tls-pw-stack*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxAWSPortalWorkerPolicy

AWSThinkboxAWSPortalWorkerPolicy 是一项 [AWS 托管策略](#)：此策略向 AWS 门户中的 Deadline Worker 授予正常操作所需的必要权限。

使用此策略

您可以将 AWSThinkboxAWSPortalWorkerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:15 UTC
- 编辑时间：2020 年 12 月 7 日 23:27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxDeadlineResourceTrackerAccessPolicy

AWSThinkboxDeadlineResourceTrackerAccessPolicy 是一项 [AWS 托管策略](#)：授予运行 AWS Thinkbox Deadline Resource Tracker 所需的权限。这包括对某些 EC2 操作的完全访问权限，包括 DeleteFleets 和 CancelSpotFleetRequests。

使用此策略

您可以将 AWSThinkboxDeadlineResourceTrackerAccessPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:25 UTC
- 编辑时间：2020 年 5 月 27 日 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxDeadlineResourceTrackerAdminPolicy

AWSThinkboxDeadlineResourceTrackerAdminPolicy 是一项 [AWS 托管策略](#)：授予创建、销毁和管理 AWS Thinkbox Deadline Resource Tracker 所需的权限。

使用此策略

您可以将 AWSThinkboxDeadlineResourceTrackerAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:29 UTC

- 编辑时间：2022 年 6 月 22 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineResourceTrackerAdminPolicy

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

AWSThinkboxDeadlineSpotEventPluginAdminPolicy 是一项 [AWS 托管策略](#)：授予 AWS Thinkbox Deadline Spot Event 插件所需的权限。这包括请求、修改和取消竞价型实例集的权限，以及有限的 PassRole 权限。

使用此策略

您可以将 AWSThinkboxDeadlineSpotEventPluginAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:38 UTC
- 编辑时间：2020 年 5 月 27 日 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 是一项 [AWS 托管策略](#)：授予 EC2 实例运行 AWS Thinkbox Deadline Spot Event Plugin Worker 软件所需的权限。

使用此策略

您可以将 AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 27 日 19:35 UTC
- 编辑时间：2020 年 12 月 7 日 23:31 UTC

- ARN: arn:aws:iam::aws:policy/
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTransferConsoleFullAccess

AWSTransferConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Transfer 的完全访问权限

使用此策略

您可以将 AWSTransferConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 12 月 14 日 19:33 UTC
- 编辑时间 : 2020 年 12 月 14 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTransferFullAccess

AWSTransferFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Transfer 服务的完全访问权限。

使用此策略

您可以将 AWSTransferFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 14 日 19:37 UTC
- 编辑时间：2020 年 12 月 14 日 19:37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTransferLoggingAccess

AWSTransferLoggingAccess 是一项 [AWS 托管策略](#)：授予 AWS Transfer 完全访问权限，以创建日志流和组并将日志事件记入您的账户

使用此策略

您可以将 AWSTransferLoggingAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 1 月 14 日 15:32 UTC
- 编辑时间：2019 年 1 月 14 日 15:32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTransferReadOnlyAccess

AWSTransferReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Transfer 服务的只读访问权限。

使用此策略

您可以将 AWSTransferReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 27 日 17:54 UTC
- 编辑时间：2020 年 8 月 27 日 17:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
{
  "Effect" : "Allow",
  "Action" : [
    "transfer:DescribeUser",
    "transfer:DescribeServer",
    "transfer:ListUsers",
    "transfer:ListServers",
    "transfer:TestIdentityProvider",
    "transfer:ListTagsForResource"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS Trusted Advisor Priority 的完全访问权限。此策略还允许用户将 Trusted Advisor 添加为具有 AWS Organizations 的受信任服务，并为 Trusted Advisor Priority 指定委派管理员账户。

使用此策略

您可以将 AWSTrustedAdvisorPriorityFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 16 日 16:08 UTC
- 编辑时间：2022 年 8 月 16 日 16:08 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS Trusted Advisor Priority 的只读访问权限。这包括查看委派管理员账户的权限。

使用此策略

您可以将 AWSTrustedAdvisorPriorityReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 16 日 16:35 UTC
- 编辑时间：2022 年 8 月 16 日 16:35 UTC
- ARN: arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTrustedAdvisorReportingServiceRolePolicy

AWSTrustedAdvisorReportingServiceRolePolicy 是一项 [AWS 托管策略](#)：适用于 Trusted Advisor 多账户报告的服务策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 19 日 17:41 UTC
- 编辑时间：2023 年 2 月 28 日 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSTrustedAdvisorServiceRolePolicy

AWSTrustedAdvisorServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Trusted Advisor 服务用于帮助降低成本、提高性能并提升 AWS 环境安全性的访问权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 2 月 22 日 21:24 UTC
- 编辑时间：世界标准时间 2024 年 1 月 18 日 16:25
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

策略版本

策略版本：v12 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSUserNotificationsServiceLinkedRolePolicy

AWSUserNotificationsServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS User Notifications 代表您调用 AWS 服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 19 日 13:28 UTC
- 编辑时间：2023 年 4 月 19 日 13:28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

AWSVendorInsightsAssessorFullAccess

AWSVendorInsightsAssessorFullAccess 是一项 [AWS 托管策略](#)：提供查看经授权的 Vendor Insights 资源和管理 Vendor Insights 订阅的完全访问权限

使用此策略

您可以将 AWSVendorInsightsAssessorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly 是一项 [AWS 托管策略](#)：提供查看经授权的 Vendor Insights 资源的只读访问权限

使用此策略

您可以将 AWSVendorInsightsAssessorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVendorInsightsVendorFullAccess

AWSVendorInsightsVendorFullAccess 是一项 [AWS 托管策略](#)：为创建和管理 Vendor Insights 资源提供完全访问权限

使用此策略

您可以将 AWSVendorInsightsVendorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2023 年 10 月 19 日 01:41 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVendorInsightsVendorReadOnly

AWSVendorInsightsVendorReadOnly 是一项 [AWS 托管策略](#)：提供查看 Vendor Insights 资源的只读访问权限

使用此策略

您可以将 AWSVendorInsightsVendorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 7 月 26 日 15:05 UTC
- 编辑时间：2022 年 12 月 1 日 00:54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVpcLatticeServiceRolePolicy

AWSVpcLatticeServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 VPC Lattice 代表您访问 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 30 日 20:47 UTC
- 编辑时间：2022 年 11 月 30 日 20:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVPCS2SVpnServiceRolePolicy

AWSVPCS2SVpnServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Site-to-Site VPN 创建和管理与您的 VPN 连接相关的资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 8 月 6 日 14:13 UTC
- 编辑时间：2019 年 8 月 6 日 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
  ]
}
```

```
}  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVPCTransitGatewayServiceRolePolicy

AWSVPCTransitGatewayServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 VPC 中转网关创建和管理中转网关 VPC 挂载的必需资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 26 日 16:21 UTC
- 编辑时间：2021 年 4 月 15 日 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSVPCVerifiedAccessServiceRolePolicy

AWSVPCVerifiedAccessServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Verified Access 服务代表您配置端点的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 29 日 03:35 UTC
- 编辑时间：世界标准时间 2023 年 11 月 17 日 21:03
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWAFConsoleFullAccess

AWSWAFConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS WAF 的完全访问权限。请注意，此策略还授予列出和更新 Amazon CloudFront 分配的权限、在

AWS Elastic Load Balancing 上查看负载均衡器的权限、查看 Amazon API Gateway REST API 和阶段的权限、列出和查看 Amazon CloudWatch 指标的权限，以及查看账户内启用的区域的权限。

使用此策略

您可以将 `AWSWAFConsoleFullAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 6 日 18:38 UTC
- 编辑时间：2023 年 6 月 5 日 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWAFConsoleReadOnlyAccess

AWSWAFConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS WAF 的只读访问权限。请注意，此策略还授予列出 Amazon CloudFront 分配的权限、在 AWS Elastic Load Balancing 上查看负载均衡器的权限、查看 Amazon API Gateway REST API 和阶段的权限、列出和查看 Amazon CloudWatch 指标的权限，以及查看账户内启用的区域的权限。

使用此策略

您可以将 AWSWAFConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 4 月 6 日 18:43 UTC
- 编辑时间 : 2023 年 6 月 5 日 20:56 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWAFFullAccess

AWSWAFFullAccess 是一项 [AWS 托管策略](#)：提供对 AWS WAF 操作的完全访问权限。

使用此策略

您可以将 AWSWAFFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 10 月 6 日 20:44 UTC
- 编辑时间：2023 年 6 月 5 日 20:55 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWAFReadOnlyAccess

AWSWAFReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 AWS WAF 操作的只读访问权限。

使用此策略

您可以将 `AWSWAFReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 10 月 6 日 20:43 UTC
- 编辑时间 : 2023 年 6 月 5 日 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

策略版本

策略版本 : v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWellArchitectedDiscoveryServiceRolePolicy

AWSWellArchitectedDiscoveryServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 WellArchitected 代表客户访问与 WellArchitected 资源相关的 AWS 服务和资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 4 月 26 日 18:36 UTC
- 编辑时间：2023 年 4 月 26 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWellArchitectedOrganizationsServiceRolePolicy

AWSWellArchitectedOrganizationsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Well-Architected 代表您访问组织。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 6 月 23 日 17:15 UTC
- 编辑时间：2022 年 7 月 25 日 18:03 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSWickrFullAccess

AWSWickrFullAccess 是一项 [AWS 托管策略](#)：此策略授予对 Wickr 服务的完全管理权限，包括 AWS Management Console 下的 Wickr 管理功能。

使用此策略

您可以将 AWSWickrFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 20:36 UTC
- 编辑时间：2022 年 11 月 27 日 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSXrayCrossAccountSharingConfiguration

AWSXrayCrossAccountSharingConfiguration 是一项 [AWS 托管策略](#)：提供管理 Observability Access Manager 链接和建立 X-Ray 跟踪共享的功能

使用此策略

您可以将 AWSXrayCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:46 UTC
- 编辑时间：2022 年 11 月 27 日 13:46 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSXRayDaemonWriteAccess

AWSXRayDaemonWriteAccess 是一项 [AWS 托管策略](#)：允许 AWS X-Ray Daemon 将原始跟踪分段数据中继到服务的 API，并检索要由 X-Ray SDK 使用的采样数据（规则、目标等）。

使用此策略

您可以将 AWSXRayDaemonWriteAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 8 月 28 日 23:00 UTC
- 编辑时间：世界标准时间 2024 年 2 月 13 日 21:58
- ARN: arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayFullAccess

AWSXrayFullAccess 是一项 [AWS 托管策略](#)：AWS X-Ray 对托管策略的完全访问权限

使用此策略

您可以将 AWSXrayFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:30 UTC
- 编辑时间：2016 年 12 月 1 日 18:30 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSXrayReadOnlyAccess

AWSXrayReadOnlyAccess 是一项 [AWS 托管策略](#)：AWS X-Ray 只读托管策略

使用此策略

您可以将 AWSXrayReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:27 UTC
- 编辑时间：世界标准时间 2024 年 2 月 14 日 00:35
- ARN: arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : [
      "*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

AWSXrayWriteOnlyAccess

AWSXrayWriteOnlyAccess 是一项 [AWS 托管策略](#)：AWS X-Ray 对托管策略的只写访问权限

使用此策略

您可以将 AWSXrayWriteOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 12 月 1 日 18:19 UTC
- 编辑时间：2018 年 8 月 28 日 23:03 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

AWSZonalAutoshiftPracticeRunSLRPolicy

AWSZonalAutoshiftPracticeRunSLRPolicy 是一项 [AWS 托管策略](#)，它：为 ARC 区域轮班练习提供管理访问权限，以及访问 CloudWatch 警报状态以监控练习运行。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 29 日 17:34
- 编辑时间：世界标准时间 2023 年 11 月 29 日 17:34
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

BatchServiceRolePolicy

BatchServiceRolePolicy 是一项 [AWS 托管策略](#)：为 AWS Batch 服务提供管理所需资源的访问权限，包括 Amazon EC2 和 Amazon ECS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 3 月 10 日 06:55 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 22:52
- ARN: arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
            ]
        }
    }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Billing

Billing 是一项 [AWS 托管策略](#)：授予账单和成本管理权限。这包括查看账户使用量，以及查看和修改预算和付款方式。

使用此策略

您可以将 Billing 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:33 UTC
- 编辑时间：世界标准时间 2024 年 1 月 17 日 18:03
- ARN: arn:aws:iam::aws:policy/job-function/Billing

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CertificateManagerServiceRolePolicy

CertificateManagerServiceRolePolicy 是一项 [AWS 托管策略](#)：Amazon Certificate Manager 服务角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 6 月 25 日 17:56 UTC
- 编辑时间：2020 年 6 月 25 日 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ClientVPNServiceConnectionsRolePolicy

ClientVPNServiceConnectionsRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Client VPN 管理您的客户端 VPN 端点连接的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 12 日 19:48 UTC
- 编辑时间：2020 年 8 月 12 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ]
    }
  ]
}
```

```
    ],  
    "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ClientVPNServiceRolePolicy

ClientVPNServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS Client VPN 管理您的客户端 VPN 端点的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 12 月 10 日 21:20 UTC
- 编辑时间：2020 年 8 月 12 日 19:39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudFormationStackSetsOrgAdminServiceRolePolicy

CloudFormationStackSetsOrgAdminServiceRolePolicy 是一项 [AWS 托管策略](#) : CloudFormation StackSets (组织主账户) 的服务角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 10 日 00:20 UTC
- 编辑时间：2019 年 12 月 10 日 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    }
  ]
}
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudFormationStackSetsOrgMemberServiceRolePolicy

CloudFormationStackSetsOrgMemberServiceRolePolicy 是一项 [AWS 托管策略](#) : CloudFormation StackSets (组织成员账户) 的服务角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型 : 服务相关角色策略
- 创建时间 : 2019 年 12 月 9 日 23:52 UTC
- 编辑时间 : 2019 年 12 月 9 日 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时 , AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudFrontFullAccess

CloudFrontFullAccess是一项[AWS托管策略](#)：提供对 CloudFront 控制台的完全访问权限以及通过列出 Amazon S3 存储桶的AWS Management Console功能。

使用此策略

您可以将 CloudFrontFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:39 UTC
- 编辑时间 : 世界标准时间 2024 年 1 月 4 日 16:56
- ARN: arn:aws:iam::aws:policy/CloudFrontFullAccess

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cfffullaccess",
      "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:*:*:*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudFrontReadOnlyAccess

CloudFrontReadOnlyAccess是一项[AWS托管策略](#)，它：提供对 CloudFront 分发配置信息和通过列出分配的访问权限AWS Management Console。

使用此策略

您可以将 CloudFrontReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：世界标准时间 2024 年 1 月 4 日 16:55
- ARN: arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudHSMServiceRolePolicy

CloudHSMServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 CloudHSM 使用或管理的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 6 日 19:12 UTC
- 编辑时间：2017 年 11 月 6 日 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams"
    ],
    "Resource" : [
      "arn:aws:logs:*:*:*"
    ]
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudSearchFullAccess

CloudSearchFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CloudSearch 配置服务的完全访问权限。

使用此策略

您可以将 CloudSearchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudSearchReadOnlyAccess

CloudSearchReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CloudSearch 配置服务的只读访问权限。

使用此策略

您可以将 CloudSearchReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC

- 编辑时间：2015 年 2 月 6 日 18:39 UTC
- ARN: arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudTrailServiceRolePolicy

CloudTrailServiceRolePolicy 是一个 [AWS 托管策略](#)，它：的权限策略 CloudTrail ServiceLinkedRole

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 10 月 24 日 21:21 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 01:18
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
      }
    }
  }
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatch-CrossAccountAccess

CloudWatch-CrossAccountAccess 是一项 [AWS 托管策略](#)：允许 CloudWatch 代表当前账户在远程账户中担任 CloudWatch-CrossAccountSharing 角色，以便跨账户、跨区域显示数据

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 7 月 23 日 09:59 UTC
- 编辑时间：2019 年 7 月 23 日 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Action" : [
      "sts:AssumeRole"
    ],
    "Resource" : [
      "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
    ],
    "Effect" : "Allow"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchActionsEC2Access

CloudWatchActionsEC2Access 是一项 [AWS 托管策略](#)：提供对 CloudWatch 警报和指标，以及 EC2 元数据的只读访问权限。提供停止、终止和重启 EC2 实例的访问权限。

使用此策略

您可以将 CloudWatchActionsEC2Access 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 7 日 00:00 UTC
- 编辑时间：2015 年 7 月 7 日 00:00 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchActionsEC2Access

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchAgentAdminPolicy

CloudWatchAgentAdminPolicy 是一项 [AWS 托管策略](#)，它具有：使用所需的全部权限 AmazonCloudWatchAgent。

使用此策略

您可以将 CloudWatchAgentAdminPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 3 月 7 日 00:52 UTC
- 编辑时间：世界标准时间 2024 年 2 月 5 日 20:59
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchAgentServerPolicy

CloudWatchAgentServerPolicy 是一个 [AWS 托管策略](#)，它： AmazonCloudWatchAgent 在服务器上使用所需的权限

使用此策略

您可以将 CloudWatchAgentServerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 3 月 7 日 01:06 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 16:37
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchApplicationInsightsFullAccess

CloudWatchApplicationInsightsFullAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Application Insights 和所需依赖项的完全访问权限。

使用此策略

您可以将 CloudWatchApplicationInsightsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 24 日 18:44 UTC
- 编辑时间：2022 年 1 月 25 日 17:51 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchApplicationInsightsReadOnlyAccess

CloudWatchApplicationInsightsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Application Insights 的只读访问权限。

使用此策略

您可以将 CloudWatchApplicationInsightsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 24 日 18:48 UTC
- 编辑时间：2020 年 11 月 24 日 18:48 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Effect" : "Allow",
    "Action" : [
      "applicationinsights:Describe*",
      "applicationinsights:List*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudwatchApplicationInsightsServiceLinkedRolePolicy

CloudwatchApplicationInsightsServiceLinkedRolePolicy 是一项 [AWS 托管策略](#) : Cloudwatch Application Insights 服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 12 月 1 日 16:22 UTC
- 编辑时间：2023 年 5 月 11 日 16:34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy

策略版本

策略版本：v24 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchApplicationSignalsServiceRolePolicy

CloudWatchApplicationSignalsServiceRolePolicy 是一项 [AWS 托管策略](#)，它：策略授予 CloudWatch 应用程序信号从其他相关 AWS 服务收集监控和标记数据的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 11 月 9 日 18:09 UTC
- 编辑时间：世界标准时间 2024 年 3 月 7 日 00:04
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  }
}
```



```
    }  
  }  
]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

CloudWatchAutomaticDashboardsAccess

CloudWatchAutomaticDashboardsAccess 是一项 [AWS 托管策略](#)：提供对用于显示 CloudWatch 自动控制面板的非 CloudWatch API 的访问权限，包括 Lambda 函数等对象的内容

使用此策略

您可以将 CloudWatchAutomaticDashboardsAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 23 日 10:01 UTC
- 编辑时间：2021 年 4 月 20 日 13:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "Version" : "2012-10-17",  
  "Statement" : [  
    {  
      "Effect" : "Allow",  
      "Action" : "cloudwatch:DescribeDashboards",  
      "Resource" : "*" }  
    ]  
}
```

```
{
  "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*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchCrossAccountSharingConfiguration

CloudWatchCrossAccountSharingConfiguration 是一项 [AWS 托管策略](#)：提供管理 Observability Access Manager 链接和建立 CloudWatch 资源共享的功能

使用此策略

您可以将 CloudWatchCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 14:01 UTC
- 编辑时间：2022 年 11 月 27 日 14:01 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
      ]
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchEventsBuiltInTargetExecutionAccess

CloudWatchEventsBuiltInTargetExecutionAccess 是一项 [AWS 托管策略](#)：允许 Amazon CloudWatch Events 中的内置目标代表您执行 EC2 操作。

使用此策略

您可以将 CloudWatchEventsBuiltInTargetExecutionAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 14 日 18:35 UTC
- 编辑时间：2016 年 1 月 14 日 18:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
```

```
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchEventsFullAccess

CloudWatchEventsFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CloudWatch Events 的完全访问权限。

使用此策略

您可以将 CloudWatchEventsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 14 日 18:37 UTC
- 编辑时间：2022 年 12 月 1 日 17:05 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchEventsInvocationAccess

CloudWatchEventsInvocationAccess 是一项 [AWS 托管策略](#)：允许 Amazon CloudWatch Events 将事件中继到您账户的 AWS Kinesis Streams 中的流。

使用此策略

您可以将 CloudWatchEventsInvocationAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2016 年 1 月 14 日 18:36 UTC
- 编辑时间：2016 年 1 月 14 日 18:36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchEventsReadOnlyAccess

CloudWatchEventsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon CloudWatch Events 的只读访问权限。

使用此策略

您可以将 CloudWatchEventsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 1 月 14 日 18:27 UTC
- 编辑时间：2022 年 12 月 1 日 16:29 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchEventsServiceRolePolicy

CloudWatchEventsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS CloudWatch 代表您执行通过警报和事件配置的操作。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 17 日 00:42 UTC
- 编辑时间：2017 年 11 月 17 日 00:42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchFullAccess

CloudWatchFullAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch 的完全访问权限。

使用此策略

您可以将 CloudWatchFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 2022 年 11 月 27 日 13:23 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccess

策略版本

策略版本 : v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchFullAccessV2

CloudWatchFullAccessV2是一个[AWS托管策略](#)，它：提供对它的完全访问权限 CloudWatch。

使用此策略

您可以将 CloudWatchFullAccessV2 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 8 月 1 日 11:32 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 19:36
- ARN: arn:aws:iam::aws:policy/CloudWatchFullAccessV2

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchInternetMonitorServiceRolePolicy

CloudWatchInternetMonitorServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Internet Monitor 代表您访问 EC2、Workspace 和 CloudFront 资源以及其他所需服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 27 日 17:46 UTC
- 编辑时间：2023 年 7 月 20 日 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchLambdaInsightsExecutionRolePolicy

CloudWatchLambdaInsightsExecutionRolePolicy 是一项 [AWS 托管策略](#) : Lambda Insights 扩展程序所需的策略

使用此策略

您可以将 CloudWatchLambdaInsightsExecutionRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略

- 创建时间：2020 年 10 月 7 日 19:27 UTC
- 编辑时间：2020 年 10 月 7 日 19:27 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchLogsCrossAccountSharingConfiguration

CloudWatchLogsCrossAccountSharingConfiguration 是一项 [AWS 托管策略](#)：提供管理 Observability Access Manager 链接和建立 CloudWatch Logs 资源共享的功能

使用此策略

您可以将 CloudWatchLogsCrossAccountSharingConfiguration 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:55 UTC
- 编辑时间：2022 年 11 月 27 日 13:55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchLogsFullAccess

CloudWatchLogsFullAccess是一项[AWS托管策略](#)，它：提供对 CloudWatch 日志的完全访问权限

使用此策略

您可以将 CloudWatchLogsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC

- 编辑时间：世界标准时间 2023 年 11 月 26 日 18:12
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudWatchLogsFullAccess",
      "Effect": "Allow",
      "Action": [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchLogsReadOnlyAccess

CloudWatchLogsReadOnlyAccess 是一项 [AWS 托管策略](#)，它：提供对 CloudWatch 日志的只读访问权限

使用此策略

您可以将 CloudWatchLogsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2015 年 2 月 6 日 18:40 UTC
- 编辑时间 : 世界标准时间 2023 年 11 月 26 日 18:11
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```



```
    }  
  ]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchNetworkMonitorServiceRolePolicy

CloudWatchNetworkMonitorServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 CloudWatch 网络监控器代表您访问和管理 EC2 和 VPC 资源、向其他必需的服务发布数据 CloudWatch 以及访问其他必需的服务。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 12 月 21 日 18:53
- 编辑时间：世界标准时间 2023 年 12 月 21 日 18:53
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchReadOnlyAccess

CloudWatchReadOnlyAccess 是一个 [AWS 托管策略](#)，它：提供对它的只读访问权限 CloudWatch。

使用此策略

您可以将 CloudWatchReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：世界标准时间 2023 年 12 月 5 日 19:24
- ARN: arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchSyntheticsFullAccess

CloudWatchSyntheticsFullAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Synthetics 的完全访问权限。

使用此策略

您可以将 CloudWatchSyntheticsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 11 月 25 日 17:39 UTC
- 编辑时间：2022 年 5 月 6 日 18:14 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess

策略版本

策略版本：v9 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CloudWatchSyntheticsReadOnlyAccess

CloudWatchSyntheticsReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Synthetics 的只读访问权限。

使用此策略

您可以将 CloudWatchSyntheticsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 11 月 25 日 17:45 UTC
- 编辑时间 : 2020 年 3 月 6 日 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComprehendDataAccessRolePolicy

ComprehendDataAccessRolePolicy 是一项 [AWS 托管策略](#)：AWS Comprehend 服务角色的策略，允许访问 S3 资源以进行数据访问

使用此策略

您可以将 ComprehendDataAccessRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2019 年 3 月 6 日 22:28 UTC
- 编辑时间：2019 年 3 月 6 日 22:28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3::*Comprehend*",
        "arn:aws:s3::*comprehend*"
      ]
    }
  ]
}
```

```
}  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComprehendFullAccess

ComprehendFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Comprehend 的完全访问权限。

使用此策略

您可以将 ComprehendFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 18:08 UTC
- 编辑时间：2017 年 12 月 5 日 01:36 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Action" : [
      "comprehend:*",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "iam:ListRoles",
      "iam:GetRole"
    ],
    "Effect" : "Allow",
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComprehendMedicalFullAccess

ComprehendMedicalFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Comprehend Medical 的完全访问权限

使用此策略

您可以将 ComprehendMedicalFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 17:55 UTC
- 编辑时间：2018 年 11 月 27 日 17:55 UTC

- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComprehendReadOnly

ComprehendReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Comprehend 的只读访问权限。

使用此策略

您可以将 ComprehendReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2017 年 11 月 29 日 18:10 UTC
- 编辑时间 : 2022 年 4 月 26 日 21:32 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendReadOnly

策略版本

策略版本 : v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComputeOptimizerReadOnlyAccess

ComputeOptimizerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 ComputeOptimizer 的只读访问权限。

使用此策略

您可以将 `ComputeOptimizerReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 3 月 7 日 00:11 UTC
- 编辑时间 : 2023 年 8 月 28 日 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ComputeOptimizerServiceRolePolicy

ComputeOptimizerServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 ComputeOptimizer 代表您调用 AWS 服务并收集工作负载详细信息。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 3 日 08:45 UTC
- 编辑时间：2022 年 6 月 13 日 19:05 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ConfigConformsServiceRolePolicy

ConfigConformsServiceRolePolicy 是一项 [AWS 托管策略](#) : AWSConfig 创建一致性包所需的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型 : 服务相关角色策略

- 创建时间 : 2019 年 7 月 25 日 21:38 UTC
- 编辑时间 : 2023 年 1 月 12 日 04:17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
}
```



```
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CostOptimizationHubAdminAccess

CostOptimizationHubAdminAccess 是一项 [AWS 托管策略](#)：此托管策略为管理员提供对成本优化中心的访问权限。

使用此策略

您可以将 CostOptimizationHubAdminAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 19 日 00:03
- 编辑时间：世界标准时间 2023 年 12 月 19 日 00:03
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]

```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CostOptimizationHubReadOnlyAccess

CostOptimizationHubReadOnlyAccess 是一项 [AWS 托管策略](#)：此托管策略提供对成本优化中心的只读访问权限。

使用此策略

您可以将 CostOptimizationHubReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 13 日 18:04
- 编辑时间：世界标准时间 2023 年 12 月 13 日 18:04
- ARN: arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CostOptimizationHubServiceRolePolicy

CostOptimizationHubServiceRolePolicy 是一项 [AWS 托管策略](#)，它：允许成本优化中心检索组织信息并收集与优化相关的数据和元数据。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：世界标准时间 2023 年 11 月 26 日 08:03
- 编辑时间：世界标准时间 2023 年 11 月 26 日 08:03

- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

CustomerProfilesServiceLinkedRolePolicy

CustomerProfilesServiceLinkedRolePolicy 是一项 [AWS 托管策略](#)：允许 Amazon Connect Customer Profiles 代表您访问 AWS 服务和资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 3 月 7 日 22:56 UTC
- 编辑时间：2023 年 3 月 7 日 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DatabaseAdministrator

DatabaseAdministrator 是一项 [AWS 托管策略](#)：授予对设置和配置 AWS 数据库服务所需的 AWS 服务和操作的完全访问权限。

使用此策略

您可以将 DatabaseAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:25 UTC
- 编辑时间：2019 年 1 月 8 日 00:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DataScientist

DataScientist 是一项 [AWS 托管策略](#)：向 AWS 数据分析服务授予权限。

使用此策略

您可以将 DataScientist 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略

- 创建时间 : 2016 年 11 月 10 日 17:28 UTC
- 编辑时间 : 2019 年 12 月 3 日 16:48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

策略版本

策略版本 : v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DAXServiceRolePolicy

DAXServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略允许 DAX 代表客户创建和管理网络接口、安全组、子网和 VPC

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 5 日 17:51 UTC
- 编辑时间：2018 年 3 月 5 日 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

DynamoDBCloudWatchContributorInsightsServiceRolePolicy 是一项 [AWS 托管策略](#)：支持 Amazon CloudWatch Contributor Insights for Amazon DynamoDB 所需的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 15 日 21:13 UTC
- 编辑时间：2019 年 11 月 15 日 21:13 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DynamoDBKinesisReplicationServiceRolePolicy

DynamoDBKinesisReplicationServiceRolePolicy 是一项 [AWS 托管策略](#)：为 AWS DynamoDB 提供对 KinesisDataStreams 的访问权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 12 日 00:43 UTC
- 编辑时间：2020 年 11 月 12 日 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

DynamoDBReplicationServiceRolePolicy

DynamoDBReplicationServiceRolePolicy 是一项 [AWS 托管策略](#)：DynamoDB 跨区域数据复制所需的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 11 月 9 日 23:55 UTC
- 编辑时间：世界标准时间 2024 年 1 月 8 日 20:10
- ARN: arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    ]
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2FastLaunchServiceRolePolicy

EC2FastLaunchServiceRolePolicy 是一项 [AWS 托管策略](#)：授予 ec2fastlaunch 在客户账户中准备和管理预先配置的快照并发布相关指标的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 1 月 10 日 13:08 UTC
- 编辑时间：2022 年 1 月 10 日 13:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2FleetTimeShiftableServiceRolePolicy

EC2FleetTimeShiftableServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略向 EC2 实例集授予将来启动实例的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 23 日 19:47 UTC
- 编辑时间：2019 年 12 月 23 日 19:47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Ec2ImageBuilderCrossAccountDistributionAccess

Ec2ImageBuilderCrossAccountDistributionAccess 是一项 [AWS 托管策略](#)：EC2 Image Builder 执行跨账户分配所需的权限。

使用此策略

您可以将 Ec2ImageBuilderCrossAccountDistributionAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 30 日 19:22 UTC
- 编辑时间：2020 年 9 月 30 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/
Ec2ImageBuilderCrossAccountDistributionAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2ImageBuilderLifecycleExecutionPolicy

EC2ImageBuilderLifecycleExecutionPolicy 是一项 [AWS 托管策略 : EC2 ImageBuilderLifecycleExecutionPolicy](#) 策略授予 Image Builder 执行诸如弃用或删除 Image Builder 图像资源及其底层资源 (AMI、快照) 等操作的权限，以支持图像生命周期管理任务的自动规则。

使用此策略

您可以将 EC2ImageBuilderLifecycleExecutionPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：世界标准时间 2023 年 11 月 16 日 23:23
- 编辑时间：世界标准时间 2023 年 11 月 16 日 23:23
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2InstanceConnect

EC2InstanceConnect 是一项 [AWS 托管策略](#)：允许客户调用 EC2 Instance Connect 向其 EC2 实例发布临时密钥并通过 ssh 或 EC2 Instance Connect CLI 进行连接。

使用此策略

您可以将 EC2InstanceConnect 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 27 日 18:53 UTC
- 编辑时间：2019 年 6 月 27 日 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```



```
{
  "Sid" : "EC2InstanceConnect",
  "Action" : [
    "ec2:DescribeInstances",
    "ec2-instance-connect:SendSSHPublicKey"
  ],
  "Effect" : "Allow",
  "Resource" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Ec2InstanceConnectEndpoint

Ec2InstanceConnectEndpoint 是一项 [AWS 托管策略](#)：用于管理客户创建的 EC2 Instance Connect 端点的 EC2 Instance Connect 端点策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 1 月 24 日 20:19 UTC
- 编辑时间：2023 年 1 月 24 日 20:19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
      ]
    }
  }
}
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2InstanceProfileForImageBuilder

EC2InstanceProfileForImageBuilder 是一项 [AWS 托管策略](#)：Image Builder 服务的 EC2 实例配置文件。

使用此策略

您可以将 EC2InstanceProfileForImageBuilder 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 12 月 1 日 19:08 UTC
- 编辑时间：2020 年 8 月 27 日 16:40 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EC2InstanceProfileForImageBuilderECRContainerBuilds

EC2InstanceProfileForImageBuilderECRContainerBuilds 是一项 [AWS 托管策略](#)：用于使用 EC2 Image Builder 构建容器映像的 EC2 实例配置文件。此策略向用户授予上传 ECR 映像的广泛权限。

使用此策略

您可以将 EC2InstanceProfileForImageBuilderECRContainerBuilds 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 12 月 11 日 19:48 UTC
- 编辑时间：2020 年 12 月 11 日 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ECRReplicationServiceRolePolicy

ECRReplicationServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 ECR Replication 使用或管理的 AWS 服务 和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 12 月 4 日 22:11 UTC
- 编辑时间：2020 年 12 月 4 日 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```



```
"Version" : "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "ecr:CreateRepository",
      "ecr:ReplicateImage"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElastiCacheServiceRolePolicy

ElastiCacheServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略 ElastiCache 允许在必要时代表您管理管理缓存所需的 AWS 资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 12 月 7 日 17:50 UTC
- 编辑时间：世界标准时间 2023 年 11 月 28 日 03:05
- ARN: arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/AmazonElasticCacheManaged" : "true"
        }
    }
},
{
    "Sid" : "ModifyVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:ModifyVpcEndpoint"
    ],
    "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
    "Condition" : {
        "StringEquals" : {
            "ec2:ResourceTag/AmazonElasticCacheManaged" : "true"
        }
    }
},
{
    "Sid" : "AllowAccessToElasticCacheTaggedVpcEndpoints",
    "Effect" : "Allow",
    "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
    ],
    "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElasticLoadBalancingFullAccess

ElasticLoadBalancingFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon ElasticLoadBalancing 的完全访问权限，以及提供 ElasticLoadBalancing 功能所需的其他服务的有限访问权限。

使用此策略

您可以将 ElasticLoadBalancingFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 9 月 20 日 20:42 UTC
- 编辑时间：2022 年 11 月 29 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
}
```

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElasticLoadBalancingReadOnly

ElasticLoadBalancingReadOnly 是一项 [AWS 托管策略](#)，它具有：提供对 Amazon ElasticLoadBalancing 和相关服务的只读访问权限

使用此策略

您可以将 ElasticLoadBalancingReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 9 月 20 日 20:17 UTC
- 编辑时间：世界标准时间 2023 年 11 月 26 日 18:15
- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalActivationsDownloadSoftwareAccess

ElementalActivationsDownloadSoftwareAccess 是一项 [AWS 托管策略](#)：查看已购买的资产，以及下载相关软件和 kickstart 文件的访问权限

使用此策略

您可以将 ElementalActivationsDownloadSoftwareAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 9 月 8 日 17:26 UTC
- 编辑时间：2020 年 9 月 8 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```



```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalActivationsFullAccess

ElementalActivationsFullAccess 是一项 [AWS 托管策略](#)：查看 Elemental Appliances and Software 购买的资产并对其采取操作的完全访问权限

使用此策略

您可以将 ElementalActivationsFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 6 月 4 日 21:00 UTC
- 编辑时间：2020 年 6 月 4 日 21:00 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "elemental-activations:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalActivationsGenerateLicenses

ElementalActivationsGenerateLicenses 是一项 [AWS 托管策略](#)：查看已购买的资产和生成待激活的软件许可证的访问权限

使用此策略

您可以将 ElementalActivationsGenerateLicenses 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 8 月 28 日 18:28 UTC
- 编辑时间：2020 年 8 月 28 日 18:28 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalActivationsReadOnlyAccess

ElementalActivationsReadOnlyAccess 是一项 [AWS 托管策略](#)：对与用户的 AWS 账户 关联的已购买资产详细列表的只读访问权限

使用此策略

您可以将 ElementalActivationsReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 8 月 28 日 16:51 UTC
- 编辑时间 : 2020 年 8 月 28 日 16:51 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalAppliancesSoftwareFullAccess

ElementalAppliancesSoftwareFullAccess 是一项 [AWS 托管策略](#)：查看 Elemental Appliances and Software 报价和订单并对其采取操作的完全访问权限

使用此策略

您可以将 ElementalAppliancesSoftwareFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 7 月 31 日 16:28 UTC
- 编辑时间：2021 年 2 月 5 日 21:01 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalAppliancesSoftwareReadOnlyAccess

ElementalAppliancesSoftwareReadOnlyAccess 是一项 [AWS 托管策略](#)：查看 Elemental Appliances and Software 报价和订单的只读访问权限

使用此策略

您可以将 ElementalAppliancesSoftwareReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 4 月 1 日 22:31 UTC
- 编辑时间：2020 年 4 月 1 日 22:31 UTC
- ARN: arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
    "Action" : [
      "elemental-appliances-software:List*",
      "elemental-appliances-software:Get*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ElementalSupportCenterFullAccess

ElementalSupportCenterFullAccess 是一项 [AWS 托管策略](#)：查看 Elemental Appliance and Software 支持案例和产品支持内容并对其采取操作的完全访问权限

使用此策略

您可以将 ElementalSupportCenterFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 11 月 25 日 18:08 UTC
- 编辑时间：2021 年 2 月 5 日 21:02 UTC
- ARN: arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

EMRDescribeClusterPolicyForEMRWAL

EMRDescribeClusterPolicyForEMRWAL 是一项 [AWS 托管策略](#)：此策略授予允许 Amazon EMR 的 WAL 服务查找并返回集群状态的只读权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 6 月 15 日 23:30 UTC
- 编辑时间：2023 年 6 月 15 日 23:30 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

FMSServiceRolePolicy

FMSServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 FM 服务相关角色在客户 AWS Organization 账户中对 FM 托管资源执行与 FM 相关的操作的访问策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 3 月 28 日 23:01 UTC
- 编辑时间：2023 年 4 月 21 日 18:33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

策略版本

策略版本：v28 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/regexpruleset/*",
      "arn:aws:wafv2:*:*:regional/regexpruleset/*"
    ]
  },
  {
    "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"
    }
  }
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

FSxDeleteServiceLinkedRoleAccess

FSxDeleteServiceLinkedRoleAccess 是一项 [AWS 托管策略](#)：允许 Amazon FSx 删除其服务相关角色以进行 Amazon S3 访问

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 28 日 10:40 UTC
- 编辑时间：2018 年 11 月 28 日 10:40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GameLiftGameServerGroupPolicy

GameLiftGameServerGroupPolicy 是一项 [AWS 托管策略](#)：允许 Gamelift GameServerGroups 管理客户资源的策略

使用此策略

您可以将 GameLiftGameServerGroupPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2020 年 4 月 3 日 23:12 UTC
- 编辑时间 : 2020 年 5 月 13 日 17:27 UTC
- ARN: arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy

策略版本

策略版本 : v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GlobalAcceleratorFullAccess

GlobalAcceleratorFullAccess 是一项 [AWS 托管策略](#)：允许 GlobalAccelerator 用户完全访问所有 API

使用此策略

您可以将 GlobalAcceleratorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 02:44 UTC
- 编辑时间：2020 年 12 月 4 日 19:17 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GlobalAcceleratorReadOnlyAccess

GlobalAcceleratorReadOnlyAccess 是一项 [AWS 托管策略](#)：允许 GlobalAccelerator 用户访问只读 API

使用此策略

您可以将 GlobalAcceleratorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 02:41 UTC
- 编辑时间：2018 年 11 月 27 日 02:41 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GreengrassOTAUpdateArtifactAccess

GreengrassOTAUpdateArtifactAccess 是一项 [AWS 托管策略](#)：提供对所有 Greengrass 区域中 Greengrass OTA 更新构件的读取访问权限

使用此策略

您可以将 GreengrassOTAUpdateArtifactAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 11 月 29 日 18:11 UTC
- 编辑时间：2018 年 12 月 18 日 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
    "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*-greengrass-updates/*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GroundTruthSyntheticConsoleFullAccess

GroundTruthSyntheticConsoleFullAccess 是一项 [AWS 托管策略](#)：此策略授予使用 SageMaker Ground Truth Synthetic 控制台所有功能所需的权限。

使用此策略

您可以将 GroundTruthSyntheticConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 25 日 15:58 UTC
- 编辑时间：2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

GroundTruthSyntheticConsoleReadOnlyAccess

GroundTruthSyntheticConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：此策略授予通过 AWS Management Console 访问 SageMaker Ground Truth Synthetic 的只读权限。

使用此策略

您可以将 GroundTruthSyntheticConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 8 月 25 日 15:58 UTC

- 编辑时间：2022 年 8 月 25 日 15:58 UTC
- ARN: arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Health_OrganizationsServiceRolePolicy

Health_OrganizationsServiceRolePolicy 是一项 [AWS 托管策略](#)：用于启用组织视图功能的 AWS Health 策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 12 月 16 日 13:28 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 16:07
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMAccessAdvisorReadOnly

IAMAccessAdvisorReadOnly 是一项 [AWS 托管策略](#)：此策略授予读取 IAM Access Advisor 提供的所有访问信息的权限，例如服务上次访问的信息。

使用此策略

您可以将 IAMAccessAdvisorReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 21 日 19:33 UTC
- 编辑时间：2019 年 6 月 21 日 19:33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMAccessAnalyzerFullAccess

IAMAccessAnalyzerFullAccess 是一项 [AWS 托管策略](#)：提供对 IAM Access Analyzer 的完全访问权限

使用此策略

您可以将 IAMAccessAnalyzerFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2019 年 12 月 2 日 17:12 UTC
- 编辑时间 : 2019 年 12 月 2 日 17:12 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMAccessAnalyzerReadOnlyAccess

IAMAccessAnalyzerReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 IAM Access Analyzer 资源的只读访问权限

使用此策略

您可以将 IAMAccessAnalyzerReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2019 年 12 月 2 日 17:12 UTC
- 编辑时间：世界标准时间 2023 年 11 月 27 日 02:24
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMFullAccess

IAMFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 IAM 的完全访问权限。

使用此策略

您可以将 IAMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2019 年 6 月 21 日 19:40 UTC
- ARN: arn:aws:iam::aws:policy/IAMFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMReadOnlyAccess

IAMReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 IAM 的只读访问权限。

使用此策略

您可以将 IAMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:40 UTC
- 编辑时间：2018 年 1 月 25 日 19:11 UTC
- ARN: arn:aws:iam::aws:policy/IAMReadOnlyAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMSelfManageServiceSpecificCredentials

IAMSelfManageServiceSpecificCredentials 是一项 [AWS 托管策略](#)：允许 IAM 用户管理自己的服务特定凭证。

使用此策略

您可以将 IAMSelfManageServiceSpecificCredentials 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 12 月 22 日 17:25 UTC
- 编辑时间 : 2016 年 12 月 22 日 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

IAMUserChangePassword

IAMUserChangePassword 是一项 [AWS 托管策略](#)：为 IAM 用户提供更改自己密码的功能。

使用此策略

您可以将 IAMUserChangePassword 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2016 年 11 月 15 日 00:25 UTC
- 编辑时间：2016 年 11 月 15 日 23:18 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    }
  ],
  {
```

```
    "Effect" : "Allow",
    "Action" : [
      "iam:GetAccountPasswordPolicy"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IAMUserSSHKeys

IAMUserSSHKeys 是一项 [AWS 托管策略](#)：让 IAM 用户能够管理自己的 SSH 密钥。

使用此策略

您可以将 IAMUserSSHKeys 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 7 月 9 日 17:08 UTC
- 编辑时间：2015 年 7 月 9 日 17:08 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserSSHKeys

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IVSFullAccess

IVSFullAccess 是一项 [AWS 托管策略](#)：提供对交互式视频服务 (IVS) 的完全访问权限，还包括完全访问 ivs 控制台所需的依赖服务的权限。

使用此策略

您可以将 IVSFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 13 日 21:20

- 编辑时间：世界标准时间 2023 年 12 月 13 日 21:20
- ARN: arn:aws:iam::aws:policy/IVSFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

IVSReadOnlyAccess

IVSReadOnlyAccess 是一项 [AWS 托管策略](#)，它：提供对 IVS 低延迟和实时流式传输 API 的只读访问权限

使用此策略

您可以将 `IVSReadOnlyAccess` 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：世界标准时间 2023 年 12 月 5 日 18:00
- 编辑时间：世界标准时间 2024 年 2 月 16 日 18:03
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

IVSRecordToS3

IVSRecordToS3 是一项 [AWS 托管策略](#)：用于执行 S3 PutObject 录制 IVS 实时流的服务相关角色

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2020 年 12 月 5 日 00:10 UTC
- 编辑时间：2020 年 12 月 5 日 00:10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

KafkaConnectServiceRolePolicy

KafkaConnectServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略授予 Kafka Connect 代表您管理 AWS 资源的权限。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 9 月 7 日 13:12 UTC
- 编辑时间：2021 年 9 月 7 日 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)

- [AWS 托管策略及转向最低权限许可入门](#)

KafkaServiceRolePolicy

KafkaServiceRolePolicy 是一项 [AWS 托管策略](#)：Kafka 的 IAM 服务相关角色策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 11 月 15 日 23:31 UTC
- 编辑时间：2023 年 4 月 28 日 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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_*"
    }
  }
}
]

```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

KeyspacesReplicationServiceRolePolicy

KeyspacesReplicationServiceRolePolicy 是一项 [AWS 托管策略](#)：Keyspaces 跨区域数据复制所需的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 5 月 2 日 16:15 UTC
- 编辑时间：2023 年 5 月 2 日 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```



```
{
  "Effect" : "Allow",
  "Action" : [
    "cassandra:Select",
    "cassandra:SelectMultiRegionResource",
    "cassandra:Modify",
    "cassandra:ModifyMultiRegionResource"
  ],
  "Resource" : "*"
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

LakeFormationDataAccessServiceRolePolicy

LakeFormationDataAccessServiceRolePolicy 是一项 [AWS 托管策略](#)：授予对 Lake Formation 资源的临时数据访问权限的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 20 日 20:46 UTC
- 编辑时间：世界标准时间 2024 年 2 月 6 日 18:37
- ARN: arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

LexBotPolicy

LexBotPolicy 是一项 [AWS 托管策略](#)：适用于 AWS Lex 自动程序使用案例的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 2 月 17 日 22:18 UTC

- 编辑时间：2019 年 11 月 13 日 22:29 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

LexChannelPolicy

LexChannelPolicy 是一项 [AWS 托管策略](#)：适用于 AWS Lex 通道使用案例的策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2017 年 2 月 17 日 23:23 UTC
- 编辑时间：2017 年 2 月 17 日 23:23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

LightsailExportAccess

LightsailExportAccess 是一项 [AWS 托管策略](#)：AWS Lightsail 服务相关角色策略，用于授予导出资源的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 9 月 28 日 16:35 UTC
- 编辑时间：2022 年 1 月 15 日 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MediaConnectGatewayInstanceRolePolicy

MediaConnectGatewayInstanceRolePolicy 是一项 [AWS 托管策略](#)：此策略授予将 MediaConnect 网关实例注册到 MediaConnect 网关的权限。

使用此策略

您可以将 MediaConnectGatewayInstanceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 3 月 22 日 20:43 UTC
- 编辑时间：2023 年 3 月 22 日 20:43 UTC
- ARN: arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MediaPackageServiceRolePolicy

MediaPackageServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 MediaPackage 将日志发布到 CloudWatch

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 9 月 18 日 17:45 UTC
- 编辑时间：2020 年 9 月 18 日 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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/*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MemoryDBServiceRolePolicy

MemoryDBServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略允许 MemoryDB 根据管理资源的需要，代表您管理 AWS 资源。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 8 月 17 日 22:34 UTC
- 编辑时间：2021 年 8 月 18 日 23:48 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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"
      }
    }
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MigrationHubDMSAccessServiceRolePolicy

MigrationHubDMSAccessServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略允许 Database Migration Service 在客户账户中担任角色以调用 Migration Hub

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 6 月 12 日 17:50 UTC
- 编辑时间：2019 年 10 月 7 日 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MigrationHubServiceRolePolicy

MigrationHubServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Migration Hub 代表您调用 Application Discovery Service

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间：2019 年 6 月 12 日 17:22 UTC
- 编辑时间：2020 年 8 月 6 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MigrationHubSMSAccessServiceRolePolicy

MigrationHubSMSAccessServiceRolePolicy 是一项 [AWS 托管策略](#)：该策略允许 Server Migration Service 在客户账户中担任角色以调用 Migration Hub

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略

- 创建时间 : 2019 年 6 月 12 日 18:30 UTC
- 编辑时间 : 2019 年 10 月 7 日 18:02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

MonitronServiceRolePolicy

MonitronServiceRolePolicy 是一项 [AWS 托管策略](#)：AWS Monitron 服务相关角色授予对所需客户资源的访问权限的策略。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 5 月 2 日 19:22 UTC
- 编辑时间：2022 年 5 月 2 日 19:22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

NeptuneConsoleFullAccess

NeptuneConsoleFullAccess 是一项 [AWS 托管策略](#)：提供使用 AWS Management Console 管理 Amazon Neptune 的完全访问权限。请注意，此策略还授予向账户内的所有 SNS 主题发布的完全访问权限，创建和编辑 Amazon EC2 实例及 VPC 配置的权限，在 Amazon KMS 上查看和列出密钥的权限以及对 Amazon RDS 的完全访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

使用此策略

您可以将 NeptuneConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2018 年 6 月 19 日 21:35 UTC
- 编辑时间：世界标准时间 2023 年 11 月 30 日 07:32
- ARN: arn:aws:iam::aws:policy/NeptuneConsoleFullAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "AllowOtherDependentPermissions",
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

NeptuneFullAccess

NeptuneFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Neptune 的完全访问权限。请注意，此策略还授予向账户内的所有 SNS 主题发布的完全访问权限和对 Amazon RDS 的完全访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

使用此策略

您可以将 NeptuneFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 30 日 19:17 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 16:32
- ARN: arn:aws:iam::aws:policy/NeptuneFullAccess

策略版本

策略版本：v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:RemoveTagsForResource",
"rds:ResetDBClusterParameterGroup",
"rds:ResetDBParameterGroup",
"rds:RestoreDBClusterFromSnapshot",
"rds:RestoreDBClusterToPointInTime",
"rds:StartDBCluster",
"rds:StopDBCluster"
],
"Resource" : [
  "*"
]
```

```
]
},
{
  "Sid" : "AllowOtherDependentPermissions",
  "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" : [
        "*"
    ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

NeptuneGraphReadOnlyAccess

NeptuneGraphReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对所有 Amazon Neptune Analytics 资源的只读访问权限以及对依赖服务的只读权限。

使用此策略

您可以将 NeptuneGraphReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：世界标准时间 2023 年 11 月 30 日 07:32
- 编辑时间：世界标准时间 2023 年 11 月 30 日 07:32
- ARN: arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:*"
    ]
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

NeptuneReadOnlyAccess

NeptuneReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Neptune 的只读访问权限。请注意，此策略还授予对 Amazon RDS 资源的访问权限。有关更多信息，请参阅 <https://aws.amazon.com/neptune/faqs/>。

使用此策略

您可以将 NeptuneReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 5 月 30 日 19:16 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 16:33
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : [
    "*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

NetworkAdministrator

NetworkAdministrator 是一项 [AWS 托管策略](#)：授予对设置和配置 AWS 网络资源所需的 AWS 服务和操作的完全访问权限。

使用此策略

您可以将 NetworkAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:31 UTC
- 编辑时间：2021 年 9 月 16 日 20:22 UTC
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

策略版本

策略版本：v11 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
}

```

```
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

OAMFullAccess

OAMFullAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Observability Access Manager 的完全访问权限

使用此策略

您可以将 OAMFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:38 UTC
- 编辑时间：2022 年 11 月 27 日 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
```

```
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "oam:*"
    ],
    "Resource" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

OAMReadOnlyAccess

OAMReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 CloudWatch Observability Access Manager 的只读访问权限

使用此策略

您可以将 OAMReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 11 月 27 日 13:29 UTC
- 编辑时间：2022 年 11 月 27 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/OAMReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

PartnerCentralAccountManagementUserRoleAssociation

PartnerCentralAccountManagementUserRoleAssociation 是一项 [AWS 托管策略](#)：提供将合作伙伴中心用户与 IAM 角色关联和取消关联的访问权限

使用此策略

您可以将 PartnerCentralAccountManagementUserRoleAssociation 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略

- 创建时间：2023 年 11 月 10 日 02:03 UTC
- 编辑时间：2023 年 11 月 10 日 02:03 UTC
- ARN: arn:aws:iam::aws:policy/
PartnerCentralAccountManagementUserRoleAssociation

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

```
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

PowerUserAccess

PowerUserAccess 是一项 [AWS 托管策略](#)：提供对 AWS 服务和资源的完全访问权限，但不允许管理用户和组。

使用此策略

您可以将 PowerUserAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 7 月 6 日 22:04 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{  
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

QuickSightAccessForS3StorageManagementAnalyticsReadOnly 是一项 [AWS 托管策略](#)：QuickSight 团队用于访问 S3 存储管理分析生成的客户数据的策略。

使用此策略

您可以将 QuickSightAccessForS3StorageManagementAnalyticsReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2017 年 6 月 12 日 18:18 UTC
- 编辑时间：2019 年 10 月 8 日 23:53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```


了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

RDSCloudHsmAuthorizationRole

RDSCloudHsmAuthorizationRole 是一项 [AWS 托管策略](#)：Amazon RDS 服务角色的默认策略。

使用此策略

您可以将 RDSCloudHsmAuthorizationRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2019 年 9 月 26 日 22:14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudhsm:CreateLunaClient",
        "cloudhsm>DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
    ],
    "Resource" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ReadOnlyAccess

ReadOnlyAccess 是一种 [AWS 托管策略](#)，它：提供对 AWS 服务和资源的只读访问权限。

使用此策略

您可以将 ReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：世界标准时间 2024 年 2 月 5 日 15:00
- ARN: arn:aws:iam::aws:policy/ReadOnlyAccess

策略版本

策略版本：v111 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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",
"ioproborunner:GetDestination",
"ioproborunner:GetSite",
"ioproborunner:GetWorker",
"ioproborunner:GetWorkerFleet",
"ioproborunner:ListDestinations",
"ioproborunner:ListSites",
"ioproborunner:ListWorkerFleets",
"ioproborunner:ListWorkers",
"iotsitewise:Describe*",
"iotsitewise:Get*",
"iotsitewise:List*",
"iotwireless:GetDestination",
"iotwireless:GetDeviceProfile",
"iotwireless:GetEventConfigurationByResourceTypes",
"iotwireless:GetFuotaTask",
"iotwireless:GetLogLevelByResourceTypes",
"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:DescribeSenderId",
"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" : "*"
}
]
```

了解更多信息

- [在 IAM Identity Center 中使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ResourceGroupsandTagEditorFullAccess

ResourceGroupsandTagEditorFullAccess 是一项 [AWS 托管策略](#)：提供对资源组和标签编辑器的完全访问权限。

使用此策略

您可以将 ResourceGroupsandTagEditorFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 8 月 10 日 13:29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

策略版本

策略版本 : v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ResourceGroupsandTagEditorReadOnlyAccess

ResourceGroupsandTagEditorReadOnlyAccess 是一项 [AWS 托管策略](#)：提供使用资源组和标签编辑器的访问权限，但不允许通过标签编辑器编辑标签。

使用此策略

您可以将 ResourceGroupsandTagEditorReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:39 UTC
- 编辑时间：2023 年 8 月 10 日 13:42 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ResourceGroupsServiceRolePolicy

ResourceGroupsServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 AWS 资源组查询拥有您资源的 AWS 服务，确保组保持最新状态

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2023 年 1 月 5 日 16:57 UTC
- 编辑时间：2023 年 1 月 5 日 16:57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAAmazonEBSCSIDriverOperatorPolicy

ROSAAmazonEBSCSIDriverOperatorPolicy 是一项 [AWS 托管策略](#)：允许 OpenShift Amazon EBS 容器存储接口 (CSI) 驱动程序操作符在 Red Hat OpenShift Service on AWS (ROSA) 集群上安装和维护 Amazon EBS CSI 驱动程序。Amazon EBS CSI 驱动程序允许 ROSA 集群管理 Amazon EBS 持久卷的生命周期。

使用此策略

您可以将 ROSAAmazonEBSCSIDriverOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:36 UTC
- 编辑时间：2023 年 4 月 20 日 22:36 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```



```
    }  
  }  
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSACloudNetworkConfigOperatorPolicy

ROSACloudNetworkConfigOperatorPolicy 是一项 [AWS 托管策略](#)：允许 OpenShift Cloud Network Config Controller Operator 配置和管理网络资源，供 Red Hat OpenShift Service on AWS (ROSA) 集群覆盖网络使用。OpenShift Cloud Network Operator 通过 CustomResourceDefinitions 代表网络插件与 AWS API 交互。Operator 使用这些策略权限来管理作为 ROSA 集群一部分的 Amazon EC2 实例的私有 IP 地址。

使用此策略

您可以将 ROSACloudNetworkConfigOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:34 UTC
- 编辑时间：2023 年 4 月 20 日 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)

- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAControlPlaneOperatorPolicy

ROSAControlPlaneOperatorPolicy 是一项 [AWS 托管策略](#)：允许 Red Hat OpenShift Service on AWS (ROSA) 控制面板管理 ROSA 集群 Amazon EC2 和 Amazon Route 53 资源。

使用此策略

您可以将 ROSAControlPlaneOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 24 日 23:02 UTC
- 编辑时间：2023 年 6 月 30 日 21:12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
      ]
    }
  }
}
```

```
}  
]  
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAImageRegistryOperatorPolicy

ROSAImageRegistryOperatorPolicy 是一项 [AWS 托管策略](#)：允许 OpenShift 映像注册操作员配置和管理 Amazon S3 存储桶和对象，供红帽 OpenShift 服务在 AWS (ROSA) 集群内映像注册表上使用，以满足 ROSA 的存储要求。OpenShift 映像注册管理器安装和维护红帽 OpenShift 集群的内部注册表。

使用此策略

您可以将 ROSAImageRegistryOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:13 UTC
- 编辑时间：世界标准时间 2023 年 12 月 12 日 19:53
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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}/*"
  ]
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAIngressOperatorPolicy

ROSAIngressOperatorPolicy 是一项 [AWS 托管策略](#)：允许 OpenShift Ingress Operator 为 Red Hat OpenShift Service on AWS (ROSA) 集群配置和管理负载均衡器和域名系统 (DNS) 配置。此策略允许读取标签值，Operator 会筛选标签值以查找 Route 53 资源，发现托管区。

使用此策略

您可以将 ROSAIngressOperatorPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:37 UTC
- 编辑时间：2023 年 4 月 20 日 22:37 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAInstallerPolicy

ROSAInstallerPolicy 是一项 [AWS 托管策略](#)：允许红帽 OpenShift 服务 AWS (ROSA) 安装程序管理支持 ROSA 群集安装的 AWS 资源。这包括管理 ROSA Worker 节点的实例配置文件。

使用此策略

您可以将 ROSAInstallerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 6 日 21:00 UTC
- 编辑时间：世界标准时间 2024 年 1 月 26 日 21:04
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
        ]
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAKMSProviderPolicy

ROSAKMSProviderPolicy 是一项 [AWS 托管策略](#)：允许内置的 ROSA AWS 加密提供程序管理 AWS Key Management Service (KMS) 密钥，以使用客户提供的 AWS KMS 密钥支持 etcd 数据加密。此策略允许使用 KMS 密钥对数据进行加密和解密。

使用此策略

您可以将 ROSAKMSProviderPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:10 UTC
- 编辑时间：2023 年 4 月 27 日 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
    "StringEquals" : {
      "aws:ResourceTag/red-hat" : "true"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAKubeControllerPolicy

ROSAKubeControllerPolicy 是一项 [AWS 托管策略](#)：允许 ROSA Kubernetes 控制器管理 ROSA 集群的 Amazon EC2、弹性负载均衡 (ELB) 和 AWS Key Management Service (KMS) 资源。

使用此策略

您可以将 ROSAKubeControllerPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 27 日 20:09 UTC
- 编辑时间：2023 年 10 月 16 日 18:17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

策略版本

策略版本：v3 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "LoadBalancerManagement",
```

```
"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" : "LoadBalancerManagementResourceTag",
  "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"
    }
  }
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAManageSubscription

ROSAManageSubscription 是一项 [AWS 托管策略](#)：此策略提供管理 Red Hat OpenShift Service on AWS (ROSA) 订阅所需的权限。

使用此策略

您可以将 ROSAManageSubscription 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2022 年 4 月 11 日 20:58 UTC
- 编辑时间：2023 年 8 月 4 日 19:59 UTC
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSANodePoolManagementPolicy

ROSANodePoolManagementPolicy 是一项 [AWS 托管策略](#)：允许 Red Hat OpenShift Service on AWS (ROSA) 将集群 EC2 实例作为 Worker 节点进行管理，包括配置安全组以及标记实例和卷的权限。此策略还允许使用 AWS Key Management Service (KMS) 密钥提供的磁盘加密的 EC2 实例。

使用此策略

您可以将 ROSANodePoolManagementPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 8 日 20:48 UTC
- 编辑时间：2023 年 6 月 8 日 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSASRESupportPolicy

ROSASRESupportPolicy 是一项 [AWS 托管策略](#)：为 ROSA 站点可靠性工程 (SRE) 提供最初观察、诊断和支持 (ROSA) 集群上与红帽 OpenShift 服务 AWS (ROSA) 相关的 AWS 资源所需的权限，包括更改 ROSA 群集节点状态的能力。

使用此策略

您可以将 ROSASRESupportPolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 6 月 1 日 14:36 UTC
- 编辑时间：世界标准时间 2024 年 1 月 22 日 22:46
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "DescribeIAMRoles",
      "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ROSAWorkerInstancePolicy

ROSAWorkerInstancePolicy 是一项 [AWS 托管策略](#)：为您账户中的 Red Hat OpenShift Service on AWS (ROSA) Worker 节点授予对 Amazon EC2 实例和计算节点生命周期管理的 AWS 区域 的只读访问权限。

使用此策略

您可以将 ROSAWorkerInstancePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2023 年 4 月 20 日 22:35 UTC
- 编辑时间：2023 年 4 月 20 日 22:35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Ec2ReadOnly",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ]
    }
  ]
}
```



```
    ],
    "Resource" : "*"
  }
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Route53RecoveryReadinessServiceRolePolicy

Route53RecoveryReadinessServiceRolePolicy 是一项 [AWS 托管策略](#)：Route 53 Recovery 就绪性的服务相关角色策略

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2021 年 7 月 15 日 16:06 UTC
- 编辑时间：2023 年 2 月 14 日 18:08 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

Route53ResolverServiceRolePolicy

Route53ResolverServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 Route53 Resolver 使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 8 月 12 日 17:47 UTC
- 编辑时间：2020 年 8 月 12 日 17:47 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

S3StorageLensServiceRolePolicy

S3StorageLensServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 S3 Storage Lens 使用或管理的 AWS 服务和资源

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2020 年 11 月 18 日 18:15 UTC
- 编辑时间：2020 年 11 月 18 日 18:15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

SecretsManagerReadWrite

SecretsManagerReadWrite是一项[AWS 托管策略](#)：通过提供对 S AWS secrets Manager 的读/写访问权限。AWS Management Console注意：这不包括 IAM 操作，因此FullAccess 如果需要轮换配置，请与 IAM 结合使用。

使用此策略

您可以将 SecretsManagerReadWrite 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 4 月 4 日 18:05 UTC
- 编辑时间：世界标准时间 2024 年 2 月 22 日 18:12
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

策略版本

策略版本：v5 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
    ]
  }
]
```

了解更多信息

- [在 IAM 身份中心使用 AWS 托管策略创建权限集](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

SecurityAudit

SecurityAudit 是一项 [AWS 托管策略](#)：安全审计模板授予读取安全配置元数据的访问权限。它对审核 AWS 账户配置的软件非常有用。

使用此策略

您可以将 SecurityAudit 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC

- 编辑时间：世界标准时间 2023 年 12 月 14 日 21:45
- ARN: arn:aws:iam::aws:policy/SecurityAudit

策略版本

策略版本：v41 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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:ListGroup",
"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"
]
}
]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

SecurityLakeServiceLinkedRole

SecurityLakeServiceLinkedRole 是一项 [AWS 托管策略](#)：此策略授予代表您操作 Amazon Security Lake 服务的权限

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2022 年 11 月 29 日 14:03 UTC
- 编辑时间：世界标准时间 2024 年 2 月 29 日 19:14
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

```
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [开始使用 AWS 托管策略，转向最低权限权限](#)

ServerMigration_ServiceRole

ServerMigration_ServiceRole 是一项 [AWS 托管策略](#)：允许 AWS Server Migration Service 将虚拟机迁移到 EC2 的权限：允许 Server Migration Service 将迁移的资源放入客户的 EC2 账户。

使用此策略

您可以将 ServerMigration_ServiceRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 8 月 11 日 20:41 UTC
- 编辑时间：2020 年 10 月 15 日 17:26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*/*"
      }
    }
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServerMigrationConnector

ServerMigrationConnector 是一项 [AWS 托管策略](#)：允许 AWS Server Migration Connector 将虚拟机迁移到 EC2 的权限。允许与 AWS Server Migration Service 通信，以及对以“sms-b-”和“import-to-ec2-”开头的 S3 桶及用于 AWS Server Migration Connector 升级、AWS Server Migration Connector 注册 AWS 和将指标上传到 AWS 的桶的读/写访问权限。

使用此策略

您可以将 ServerMigrationConnector 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2016 年 10 月 24 日 21:45 UTC
- 编辑时间 : 2016 年 10 月 24 日 21:45 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationConnector

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServerMigrationServiceConsoleFullAccess

ServerMigrationServiceConsoleFullAccess 是一项 [AWS 托管策略](#)：使用 Server Migration Service 控制台所有功能所需的权限

使用此策略

您可以将 ServerMigrationServiceConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2020 年 5 月 9 日 17:18 UTC
- 编辑时间：2020 年 7 月 20 日 22:00 UTC
- ARN: arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServerMigrationServiceLaunchRole

ServerMigrationServiceLaunchRole 是一项 [AWS 托管策略](#)：允许 AWS Server Migration Service 在客户的 AWS 账户中创建和更新相关 AWS 资源，以启动迁移的服务器和应用程序的权限。

使用此策略

您可以将 ServerMigrationServiceLaunchRole 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2018 年 11 月 26 日 19:53 UTC
- 编辑时间：2020 年 10 月 15 日 17:29 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
}

```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServerMigrationServiceRoleForInstanceValidation

ServerMigrationServiceRoleForInstanceValidation 是一项 [AWS 托管策略](#)：允许 AWS SMS 运行使用的数据验证脚本并将脚本成功/失败发送回 SMS 的权限

使用此策略

您可以将 `ServerMigrationServiceRoleForInstanceValidation` 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2020 年 7 月 20 日 22:25 UTC
- 编辑时间：2020 年 7 月 20 日 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServiceQuotasFullAccess

ServiceQuotasFullAccess 是一项 [AWS 托管策略](#)：提供对 Service Quotas 的完全访问权限

使用此策略

您可以将 ServiceQuotasFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 24 日 15:44 UTC
- 编辑时间：2021 年 2 月 4 日 21:29 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasFullAccess

策略版本

策略版本：v4 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
    }
  }
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServiceQuotasReadOnlyAccess

ServiceQuotasReadOnlyAccess 是一项 [AWS 托管策略](#)：提供对 Service Quotas 的只读访问权限

使用此策略

您可以将 ServiceQuotasReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 6 月 24 日 15:31 UTC
- 编辑时间：2020 年 12 月 21 日 18:11 UTC

- ARN: arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ServiceQuotasServiceRolePolicy

ServiceQuotasServiceRolePolicy 是一项 [AWS 托管策略](#)：允许 Service Quotas 代表您创建支持案例

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 5 月 22 日 20:44 UTC
- 编辑时间：2019 年 6 月 24 日 14:52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

SimpleWorkflowFullAccess

SimpleWorkflowFullAccess 是一项 [AWS 托管策略](#)：提供对 Simple Workflow 配置服务的完全访问权限。

使用此策略

您可以将 SimpleWorkflowFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2015 年 2 月 6 日 18:41 UTC
- 编辑时间：2015 年 2 月 6 日 18:41 UTC
- ARN: arn:aws:iam::aws:policy/SimpleWorkflowFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

SupportUser

SupportUser 是一项 [AWS 托管策略](#)：此策略授予在 AWS 账户 中排查和解决问题的权限。此策略还允许用户联系 AWS 支持以创建和管理案例。

使用此策略

您可以将 SupportUser 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:21 UTC
- 编辑时间：2023 年 8 月 25 日 18:40 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

策略版本

策略版本：v8 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

SystemAdministrator

SystemAdministrator 是一项 [AWS 托管策略](#)：授予对应用程序和开发操作所需的必要资源的完全访问权限。

使用此策略

您可以将 SystemAdministrator 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:23 UTC
- 编辑时间：2020 年 8 月 24 日 20:05 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

策略版本

策略版本：v6 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

TranslateFullAccess

TranslateFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon Translate 的完全访问权限。

使用此策略

您可以将 TranslateFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 27 日 23:36 UTC
- 编辑时间：2020 年 1 月 8 日 21:22 UTC
- ARN: arn:aws:iam::aws:policy/TranslateFullAccess

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

TranslateReadOnly

TranslateReadOnly 是一项 [AWS 托管策略](#)：提供对 Amazon Translate 的只读访问权限。

使用此策略

您可以将 TranslateReadOnly 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2017 年 11 月 29 日 18:22 UTC
- 编辑时间：2023 年 5 月 24 日 17:19 UTC
- ARN: arn:aws:iam::aws:policy/TranslateReadOnly

策略版本

策略版本 : v7 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

ViewOnlyAccess

ViewOnlyAccess 是一项 [AWS 托管策略](#)：此策略授予查看所有 AWS 服务的资源和基本元数据的权限。

使用此策略

您可以将 ViewOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：工作职能策略
- 创建时间：2016 年 11 月 10 日 17:20 UTC
- 编辑时间：2023 年 3 月 6 日 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

策略版本

策略版本：v17 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

VMImportExportRoleForAWSConnector

VMImportExportRoleForAWSConnector 是一项 [AWS 托管策略](#)：VM Import/Export 服务角色的默认策略，适用于使用 AWS Connector 的客户。此策略让 VM Import/Export 服务承担角色，满足 AWS Connector 虚拟设备的虚拟机迁移请求。（请注意，AWS Connector 使用“AWSConnector”托管策略代表客户向 VM Import/Export 服务发出请求。）提供创建 AMI 和 EBS 快照、修改 EBS 快照属性、对 EC2 对象进行“描述*”调用以及从以“import-to-ec2”开头的 S3 桶进行读取的功能。

使用此策略

您可以将 VMImportExportRoleForAWSConnector 附加到您的用户、组和角色。

策略详细信息

- 类型：服务角色策略
- 创建时间：2015 年 9 月 3 日 20:48 UTC
- 编辑时间：2015 年 9 月 3 日 20:48 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

VPCLatticeFullAccess

VPCLatticeFullAccess 是一项 [AWS 托管策略](#)：提供对 Amazon VPC Lattice 的完全访问权限和对依赖项服务的访问权限。

使用此策略

您可以将 VPCLatticeFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:49 UTC
- 编辑时间：2023 年 3 月 30 日 02:49 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeFullAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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"
  }
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

VPCLatticeReadOnlyAccess

VPCLatticeReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 Amazon VPC Lattice 的只读访问权限和对依赖项服务的有限访问权限。

使用此策略

您可以将 VPCLatticeReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:47 UTC
- 编辑时间：2023 年 3 月 30 日 02:47 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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" : "*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

VPCLatticeServicesInvokeAccess

VPCLatticeServicesInvokeAccess 是一项 [AWS 托管策略](#)：提供调用 Amazon VPC Lattice 服务所需的访问权限。

使用此策略

您可以将 VPCLatticeServicesInvokeAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2023 年 3 月 30 日 02:45 UTC
- 编辑时间：2023 年 3 月 30 日 02:45 UTC

- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WAFLoggingServiceRolePolicy

WAFLoggingServiceRolePolicy 是一项 [AWS 托管策略](#)：创建 SLR 以将客户日志写入 Firehose 流

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 24 日 21:05 UTC
- 编辑时间：2018 年 8 月 24 日 21:05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WAFRegionalLoggingServiceRolePolicy

WAFRegionalLoggingServiceRolePolicy 是一项 [AWS 托管策略](#)：创建 SLR 以将客户日志写入 Firehose 流

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2018 年 8 月 24 日 18:40 UTC
- 编辑时间：2018 年 8 月 24 日 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

```
    }  
  ]  
}
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WAFV2LoggingServiceRolePolicy

WAFV2LoggingServiceRolePolicy 是一项 [AWS 托管策略](#)：此策略会创建服务相关角色，允许 AWS WAF 向 Amazon Kinesis Data Firehose 写入日志。

使用此策略

此附加到服务相关角色的策略允许服务代表您执行操作。您无法将此策略附加到您的用户、组或角色。

策略详细信息

- 类型：服务相关角色策略
- 创建时间：2019 年 11 月 7 日 00:40 UTC
- 编辑时间：2020 年 7 月 23 日 17:04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy

策略版本

策略版本：v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
```

```
"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" : "*"
  }
]
```

了解更多信息

- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WellArchitectedConsoleFullAccess

WellArchitectedConsoleFullAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Well-Architected Tool 的完全访问权限

使用此策略

您可以将 WellArchitectedConsoleFullAccess 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2018 年 11 月 29 日 18:19 UTC
- 编辑时间：2018 年 11 月 29 日 18:19 UTC

- ARN: arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess

策略版本

策略版本 : v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WellArchitectedConsoleReadOnlyAccess

WellArchitectedConsoleReadOnlyAccess 是一项 [AWS 托管策略](#)：提供通过 AWS Management Console 访问 AWS Well-Architected Tool 的只读访问权限

使用此策略

您可以将 WellArchitectedConsoleReadOnlyAccess 附加到您的用户、组和角色。

策略详细信息

- 类型 : AWS 托管策略
- 创建时间 : 2018 年 11 月 29 日 18:21 UTC
- 编辑时间 : 2023 年 6 月 29 日 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

策略版本

策略版本 : v2 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

WorkLinkServiceRolePolicy

WorkLinkServiceRolePolicy 是一项 [AWS 托管策略](#)：允许访问 AWS 服务以及 Amazon WorkLink 使用或管理的资源

使用此策略

您可以将 WorkLinkServiceRolePolicy 附加到您的用户、组和角色。

策略详细信息

- 类型：AWS 托管策略
- 创建时间：2019 年 1 月 23 日 19:03 UTC
- 编辑时间：2019 年 1 月 23 日 19:03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

策略版本

策略版本：v1 (默认)

此策略的默认版本是定义策略权限的版本。当使用该策略的用户或角色请求访问 AWS 资源时，AWS 会检查策略的默认版本以确定是否允许该请求。

JSON 策略文档

```
{
  "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-*"
}
]
```

了解更多信息

- [Create a permission set using AWS managed policies in IAM Identity Center](#)
- [添加和删除 IAM 身份权限](#)
- [了解 IAM policy 版本控制](#)
- [AWS 托管策略及转向最低权限许可入门](#)

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。